6.805 Class 4, Sept. 27: Copyright

Class 3, Sept. 27, 2012 - Introduction to Copyright Law and Application to the Digital, Networked World

6.805: Foundations of Internet Policy - Semester Calendar

Goals

This is an introduction to copyright law, looking at the roots of copyright protection as a property right, understanding the basics of what copyright protects, and then exploring the challenges of applying copyright law to digital content and the Internet.

Class Preparation

WARNING - There is a lot to read here. Do not try to do it all in Wednesday night!

Read and be sure to understand each statute and case referenced here. There is no writing assignment this week because there is a lot of reading. This class serves as the foundation for our discussion of SOPA and PIPA that will come later in the semester.

- Overview
  - Larry Lessig, Presentation to the O'Reilly Open Source Conference (July 2002).
  - Read Excerpts from Robert Levine, Free Ride
- The Law:
  - The 1891 case from the Colorado Supreme Court, *Strickler v. City of Colorado Springs* (16 Colo. 61; 26 P. 313; 1891 Colo. LEXIS 158). This deals with the rights of a landowner to water flowing through his property — so-called *riparian rights*. It raises basic issues of what property is and serves as a useful foil to our discussion of intellectual property policy. Read this short case.
  - Read these sections of the Copyright Act: 17 USC §§ 102, 106, 107 The complete Copyright Law is massive, but read these key sections.
  - Read the Supreme Court case Baker v. Selden, 101 U.S. 99 (1879), in which the Court ruled that describing a system of accounting in a textbook did not confer copyright protection on the system itself. This is a major precedent in copyright law concerning the *idea/expression doctrine*.
  - Read the Supreme Court ruling in *Sony Corporation of America v. Universal City Studios*, and brief the case. The brief is for you, not for turning in. But you'll need the brief in order to participate in the class.
- Online Copyright liability:
  - Read sections of the Digital Millenium Copyright Act: 17 USC § 512 - Sections (a)-(d)
  - Read the first test of the DMCA, Universal Studios v. Corley, 273 F.3d 429 (CA2, 2001)
  - Read Viacom International v. YouTube, 676 F.3d 19 (2d Cir. 2012). (Second Court ruling Viacom's appeal of District Court's ruling in favor of YouTube's request for summary judgment in Viacom's $1 billion lawsuit.)

Starting the term projects

This week we'll start the class term projects. There will be project milestones throughout the rest of the semester. See the project information and schedule of milestones.

For class on September 27, we will ask you form teams and pick topics, so you should be prepared to do that.

6.805 Semester Projects

6.805 Semester Projects

The major factor in your semester grade will be your team project: an analysis of an important topic in the internet policy agenda of the next administration. Don't think of this a class term paper. Rather, it should be an example of the best policy thinking of of some of the best technically informed upcoming leaders of the next decade: you. You should aim to produce a work that you would be happy to have associated with your name and to be distributed to people in government and in the Internet policy world -- and the course staff might do just that.

Teams should have four members. Each team will work with a mentor who is an internet policy expert. It will be your responsibility to arrange meetings with your mentor, typically by phone or video. Each team will also have members of the 6.805 staff assigned to help with policy and with writing.

Keep in mind that we require good quality writing. Papers with spelling, grammatical, or stylistic errors will be penalized in grading, or might even not be accepted. Good resources on writing are The Mayfield Handbook of Technical and Scientific Writing, by Les Perelman, Ed Barrett, and Jim Paradis, and Grammar and Style Notes by Jack Lynch.

Model papers

The paper doesn't have to be long: even 30-40 pages might be adequate. But it does need to be thoroughly researched, with sufficient background to support your analysis and recommendations. The fact that you make will recommendations doesn't mean that this should be an pure advocacy piece. Rather it should provide a sound analysis of alternative options and discuss pros and cons, and typically end up recommending some alternatives over others.

Here a couple of papers to use as exemplars of the kind of thing work we're looking for:

- President's Council of Advisors on Science and Technology Spectrum Policy Report
- Consumer Privacy Bill of Rights - The White House
- Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill
- Enabling Trade in the Era of Information Technologies: Breaking Down Barriers to the Free Flow of Information

These are, of course, professionally produced but they do reflect that level of seriousness that we expect from your writing.

Research

We expect you to do thorough research on your topic, with extensive references. News reports, webzine articles, and Wikipedia can be good ways to get started, but make sure to not stop there: go to primary sources. If you're doing anything even remotely about legal issues, you should make sure to

check out law review papers, which can be searched from MIT through LexisNexis Academic Legal Reviews. You'll need to have MIT certificates installed in your browser. And it really helps to interview people who are directly involved with the topic you are writing about.

Suggested Topics

We suggest that you chose a paper topic from among these broad subject areas. Each one of these will be far too broad to cover in its entirety, but do give you a sense of relevant topics on which you can do useful research.

1. Commercial privacy
2. Cybersecurity
3. Updating Electronic Surveillance Law
4. Global online free flow of information and trade
5. Global Internet governance
6. Online copyright
7. Broadband adoption and deployment

If your team comes up with another topic, we are certainly open to discussion.

Schedule

Here is the schedule of milestones for your paper, to help you plan. More detailed information about each assignment will be posted as the due dates come closer.

- **Sept. 27** Pick topics and form teams: For homework, each team should turn in a page saying what you think you want to investigate and how you propose to go about it, with a few selected references. Turn in a one-page description of the issue you plan to investigate in your paper, and how you propose to go about this. Course staff will help with picking mentors.
- **Oct. 4:** Mentors assignments and topics finalized.
- **Oct. 11:** Each team presents its plan for doing research, including a problem statement, writing, and schedule for meeting with mentors. Each team should also present a plan for how they will divide up the work. One person on the team needs to be selected as the report editor, and will have overall responsibility for the final product.
- **Oct. 18:** Each team does 3-minute oral presentation in class on on topic, preliminary directions, and work plan.
- **Oct. 25:** Due for homework: Report outline: What's the problem? What are possible solutions? Why is our solution better than other solutions? What are arguments against our solution? Proposed bibliography
- **Nov. 1:** There will be an individual writing assignment on another topic. Staff meetings with teams to review progress.
- **Nov. 8:** First draft due from each team: It should be full-length and fully researched. There will be an assignment for each team to critique another team's draft and argue against their proposal.
- **Nov. 15:** Oral presentations in class.
- **Nov. 29:** Revised draft due. **No extensions.**
- **Dec. 12:** Final paper due. **No extensions.**

Billboard.biz

Universal Struck Gold With PolyGram Merger in 1998, Can They Do It With EMI?

AEG CEO Tim Leiweke On Impending Sale: 'We Won't Miss a Beat'

Universal-EMI Merger: A Timeline Of Events

Business Matters: No Ceiling in Sight for Subscription Services

Backbeat: Michael Kiwanuka Wows Webster Hall, John Mayer, Kierszenbaum

Must-Read Excerpt From Robert Levine's 'Free Ride: How Digital Parasites Are Destroying the Culture Business and How the Culture Business Can Fight Back'

November 02, 2011 | By Robert Levine

[Not] Paid In Full: Why Creators Must Reassert Their Rights In The Information Economy

Piracy isn't just draining record-label revenue-it's threatening the economic viability of creating content. In his new book, "Free Ride: How Digital Parasites Are Destroying the Culture Business, and How the Culture Business Can Fight Back" (Doubleday), former Billboard executive editor Robert Levine provides a rejoinder to the Silicon Valley cliché that "information wants to be free." As he points out, "The information that wants to be free is almost always the information that belongs to someone else."

In "Free Ride," Levine outlines how boardroom and courtroom battles have shaped the dysfunctional online media business. He chronicles the passage of the Digital Millennium Copyright Act, examines the rise of Napster and YouTube and reports on Google's role in funding advocacy groups that lobby against intellectual property protections. He also takes a look at how the same problems decimating the recording industry are also hurting newspapers, TV networks, book publishers and movie studios.

In an excerpt from his concluding chapter, Levine breaks down the challenges facing the culture business-and suggests survival tactics:

The Internet has been so open for so long that many people just assume its structure is the inevitable result of the technological advances that created it. That's not really the case. Technology makes certain things inevitable: broadband speeds will get faster, computers will get more powerful, and almost everything related to either one will get cheaper. But it doesn't dictate how engineers set up the resulting networks, much less how politicians regulate them. Those are our choices. And fully closed or fully open networks would be the worst two choices we could make.

Most Popular Most emailed

Articles Clicking a tab sets your default view

- Universal-EMI Merger: A Timeline Of Events
- Live Nation, TicketMaster, StubHub Apps Add Support For Apple's New Passbook | Billboard.biz
- Country, AC Lead Music Formats at 2012 Marconi Awards
- Universal Music-EMI Merger: UMG Struck Gold With PolyGram in the 1990s, Can They Do It Again?
- Chart Moves: 'Glee' Returns to Billboard Hot 100, Lil Wayne Ties Elvis Presley's Record | Billboard.biz
- Universal Music's Acquisition of EMI Approved by Federal Trade Commission | Billboard.biz
- Chart Moves: 'Fifty Shades of Grey' Album Debuts on Billboard 200 Chart, David Byrne Hits New High | Billboard.biz
- Universal Music CEO Lucian Grainge on Owning EMI, Growing Capitol and Virgin, and Losing Parlophone
- FAQ on Approval of Universal Music - EMI Deal
- Led Zeppelin's Robert Plant, Jimmy Page, John Paul Jones Regroup for DVD Press Conference, Not Tour | Billboard.biz

Washington helped create the Internet as it exists today, by passing the Digital Millennium Copyright Act (DMCA), letting the Internet operate freely across borders, and encouraging the growth of online commerce in a variety of ways. In the next few years, a series of regulatory decisions coming to a head there and in other capitals will either lock in the status quo or open the possibility of change. Among the most important decisions are on "net neutrality": proposals that would forbid Internet service providers from favoring some services and sites or slowing down others. Other decisions involve how much control companies like Apple can exercise over how their devices interact with the Internet and whether the United States can block Web sites that violate its laws. Although online companies play up the idea of keeping the Internet "unregulated," establishing this openness would actually require regulating Internet service providers, device makers and other companies. For all their talk of innovation, Google and other technology giants have the same agenda as the media companies and Internet service providers they lobby against: regulation for thee but not for me.

Online activists present the choice about our online future as one between control and creativity, but it's really about commerce or chaos. A completely closed system would indeed defeat the purpose of the Internet; it would limit both commerce and creativity. But so would an absolutely open one, where selling digital media-or anything that can be reduced to zeros and ones-would be almost impossible in the long run. We'd have a 21st-century communications infrastructure supporting a 17th-century economy, where artists need patrons and only physical items have value. That doesn't sound like progress.

iTunes

In fact-although reports of its death have been greatly exaggerated-one reason for the Web's decline relative to the app world is the fact that it's hard to sell media there and even harder to make money giving it away. Condé Nast, which owns Wired, seems to agree. An iPad app of the magazine's June 2010 issue sold more than 100,000 copies-more than its print counterpart, for the same $4.99 price. The magazine gets 70% of that, plus advertising revenue. And although apps based on subsequent issues sold fewer copies, publishers are still learning how to build appealing apps, and the iPad is still growing as a platform. Condé Nast saw so much potential in Apple's device that it made the Wired app designer, Scott Dadich, its VP of digital magazine development. Suddenly, it seems, the future involves paying for stuff.

well at start

But that future can come about only if there's an effective way to make sure more stuff is paid for than taken. That means revisiting or interpreting the DMCA to give Internet service providers, online locker services, and ad networks at least some responsibility for how their products are used. As Congress recognized at the time, it would be impractical for Internet service providers to have legal responsibility for everything they carry on their networks. But it seems increasingly irresponsible for them to do nothing. The way some Web sites and online locker services maintain willful ignorance about copyright infringement-arguing that it's someone else's problem-is no way to run a legitimate business. Giving safe harbor if they use a basic level of filtering, as YouTube does now, would be a reasonable compromise. This wouldn't slow innovation; it would encourage it. As pirate sites lost their unfair advantage, legitimate services would attract more investment and prosper. Online companies could try to make things better, not just cheaper.

Questions about the future of the online world are becoming more urgent as consumers connect televisions and other devices to the Internet. For now, film and television companies still count on a steady stream of revenue from cable, a closed system that makes piracy impractical. But devices like Google TV will increasingly bring the Internet into the living room-online locker services, Russian pirate movie sites, and all. In order to preserve the free-for-all that helps them thrive, technology companies are promoting regulations that would nearly forbid Internet service providers to stop them. "We need to be conservative in this debate and preserve what has worked in driving this economy," Lawrence Lessig said at an April 2008 Federal Communications Commission hearing, "and what has worked is a neutral network."

But this status quo works far better for technology companies than for creators. If a country had a market where about a quarter of all commerce was illegal and the rest was dominated by a few large companies, no one would call that economy a success. You can't have a functioning economy without a market, you can't have a market without some form of property rights, and those rights don't mean anything if they can't be enforced. Do we really want to risk destroying a centuries-old market for cultural products to ensure that the Internet can continue to work the way it did in 1995?

GOOGLE AND THE PUBLIC ADVOCACY organizations allied with it promote the idea of an "open Internet," which refers to several loosely intertwined ideas, including net neutrality and an absence of barriers to the exchange of data. The goal of an open Internet is promoted as a progressive idea, and the phrase is filled with positive associations: After all, who doesn't want to be open? Public advocacy groups say this openness is the key to preserving free expression online, but it allows corporations as well as people to act as they wish, which isn't progressive at all. On an Internet of

is progressive - yes

but realistic

sites that exchange data without restrictions, the information that wants to be free could include a record of everything you've ever done online. These notions of open and closed aren't absolutes, of course; it makes more sense to think of them as points on a continuum. Both have their advantages. Linux, the open-source operating system, has both flexibility and power. Wikipedia, the ultimate open media product, is a fantastic tool for accessing information. And crowdsourcing journalism that involves combing through massive amounts of data has been very effective.

Closed systems seem better suited to commerce, though. It's one reason DVDs became such a moneymaker for Hollywood studios. It's why video game publishers have cut investment in PC titles to focus on closed consoles like Microsoft's Xbox 360 and Nintendo's Wii. (The most successful PC game of recent years, World of Warcraft, is a closed system of its own; it charges a subscription fee.) And it's why apps sell much better for Apple's iPhone platform than for Google's Android operating system. The online world needs to support both.

THE LONGER THE CURRENT ONLINE CHAOS LASTS, the more bitter the fight between creators and copyright infringers gets. In December 2008, the RIAA announced it would stop suing individual uploaders in favor of finding a way to cut piracy by cooperating with Internet service providers. But a few small film studios and porn producers have retained lawyers to file copyright infringement lawsuits against individuals, seemingly as a moneymaking venture. From early 2010 to January 2011, a law firm called the U.S. Copyright Group filed almost 100,000 lawsuits against U.S. residents who had uploaded films such as "The Hurt Locker" and "Far Cry," and then sent letters offering to settle for $1,500. While creators have the right to seek redress for infringement, these mass suits are turning the justice system into a reverse lottery that addresses widespread losses by trying to collect absurd amounts of money from an unlucky few. Several organizations, including the Electronic Frontier Foundation, have lined up to help fight the suits, most of which will probably end up being dismissed for jurisdictional or technical reasons.

Copyright laws do need to be revised to bring some order to the Internet; we need shorter terms of protection, a way to take quicker action against commercial-scale pirates, and less draconian damages for individual infringers. Specifically, a small-claims court for copyright infringement would allow independent artists to assert their rights without burdening the court system and distinguish casual downloaders from moneymaking operations. To deal with the former, it's much fairer to sue 100,000 illegal downloaders for $50 each than it is to sue 50 users for $100,000 each, and the law should make that possible. Making such suits an unpleasant but routine event-like getting a speeding ticket-would cut down on infringement as well.

Passing new laws will be difficult: copyright holders know the current level of potential damages gives them negotiating leverage with technology companies, and online activists still hope to legalize file sharing. For the near future at least, the fight will be over how-or even if-the copyright laws we already have will be enforced. And for all the Obama administration's admiration for Google, Hollywood has enormous influence with the Democrats, and Vice President Joe Biden has always championed the protection of intellectual property. In June 2010, Biden threw down the gauntlet at a press conference and said, "Piracy is theft." He appeared with Victoria Espinel, a former negotiator in the Office of the U.S. Trade Representative, whom President Barack Obama had appointed the first "copyright czar." In a report released that day, Espinel introduced a strategy to fight online piracy and trafficking in counterfeit goods that focuses on interagency cooperation and an insistence on seeing infringement-along with patent and trademark violations-as an issue that negatively affects several sectors of the U.S. economy. (Formally, Espinel holds the title of U.S. intellectual property enforcement coordinator, with a purview that extends to patents, trademarks, and counterfeit goods off-line as well as on the Internet.) Espinel's report also recommended cooperating more extensively with foreign governments and, in a significant nod to fair use, asserted that "strong intellectual property enforcement efforts should be focused on stopping those stealing the work of others, not those who are appropriately building upon it."

Espinel, who has won respect in both Hollywood and Silicon Valley-no small feat-doesn't think we have to choose between the media business and the Internet. "One of the things that I'm trying to avoid is having people view policies-net neutrality is a good example-as creating a conflict with intellectual property enforcement," she says. "There's this view that the administration has two policy goals-one is to keep the Internet open and accessible, and the other is to enforce intellectual property laws-and one of those needs to be sacrificed for the benefit of the other. That's not my view, and I think we should be able to move forward and accomplish both of those goals, and I think that's true in a number of areas."

But some technology executives seem to resent the idea that copyright laws will be enforced at all. Many mocked Espinel's report, which said movie and video piracy cost the U.S. economy $20.5 billion a year. (The number is probably exaggerated, but even a quarter of that would be way too much.) Michael Arrington, the founder of the TechCrunch blog, wrote about an off-the-record meeting he attended between Espinel and several top technology executives and complained that "Espinel

has a single agenda when it comes to copyright issues." But that agenda is enforcing the law. According to his post, Espinel reminded him, "My job title is Intellectual Property Enforcement after all."

WHATEVER HAPPENS, the future won't be what it used to be.

Back in 1993, almost everyone predicted the information superhighway would be a huge boon to the culture business. Good jobs would be created by new opportunities to sell music, movies, and other forms of entertainment still being developed. Independent artists would be able to sell their work without studios or labels. Media would improve in quality, as well as quantity.

The Internet has brought forth many wonders, from the silly to the sublime to the skateboarding bulldog on YouTube (which is both). Newspapers no longer have a monopoly on serious journalism, and their mistakes are promptly challenged. Anyone can create culture instead of simply consuming it. It's never been easier to distribute creative work. At the same time, it's never been harder to get paid for it.

The Internet has been an impressive engine of economic growth. But a great deal of that growth has gone to a small number of technology companies. They depend on informative journalism to make their search engines useful, and they depend on compelling music and movies to make digital players worth owning. But the companies that fund those cultural products have never been in worse shape. They're cutting jobs, and with them the ability to create and market new work. Those search engines and players won't be nearly as valuable without them.

The current situation is slowly robbing the Internet of its potential. Rather than encourage innovation and excellence, it rewards cost cutting and crowdsourcing. The effects can be underwhelming. In his book "You Are Not a Gadget: A Manifesto," the computer scientist Jaron Lanier points out that two of the most widely acclaimed results of the remarkable technological advances of the Internet are Wikipedia and Linux, a free encyclopedia and a new version of the Unix operating system.

We can do better.

No one believes that piracy could be stopped by a law like the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property (PROTECT IP) Act or the agreement in July between media companies and Internet service providers. And even stopping it completely wouldn't solve all of the culture businesses' problems. But regulations like these, whether private or public, would allow a working market to emerge. Creators would sell, consumers would buy and both would benefit. Music and movie companies will probably never enjoy the kinds of profit margins they did in the 1990s, but they could return to stability by persuading creators that they still have value in a world of digital distribution. Artists would have the option of working with big companies or making their own way in an online economy that allowed them to do business, not just take donations.

In a functioning market, online media would get better, not just cheaper. And this, in turn, would fuel the growth of more technology companies. This wouldn't break the Internet; it would help it live up to its potential.

....

From "Free Ride: How Digital Parasites Are Destroying the Culture Business, and How the Culture Business Can Fight Back" by Robert Levine. Published by arrangement with Doubleday, an imprint of Knopf Doubleday Publishing Group, a division of Random House. It was published Oct. 25.

new biz models + services

how much has rev actually L

(would have never asked before soph yr)

PIPA

So what is he really saying?

v

TAGS: **Record Labels Publishing Digital & Mobile Legal & Management**

Comments for this page are closed.

Showing 7 comments Sort by popular now

Yeah Right

Grossly misinformed at best.

N.

stazie

Very timely. The future indeed cannot be the same much longer.

Tom

Really amazing book.

Julián Landerreche

"(...) two of the most widely acclaimed results of the remarkable technological advances of the Internet are Wikipedia and Linux, a free encyclopedia and a new version of the Unix operating system."

I agree.

But then you wrote:

"We can do better."

What exactly can we do better? Name it, list it, please.Or are you tacitly talking about 3D movies and pop music?

juepucta

"The old world is dead, the new world is yet to be born, and in the interregnum there is much morbidity". - Gramsci

Don-dirko

So, let's start with your life, wild west is back, laws won't be needed anymore

nina

great read. In the book he goes even deeper into the google power-network. Stuff nobody has written about before.

Trackback URL http://disqus.com/forums/bi

blog comments powered by DISQUS

SAVE | EMAIL | PRINT | RSS | REPRINTS

STRICKLER v. CITY OF COLORADO SPRINGS.

Supreme Court of Colorado

16 Colo. 61; 26 P. 313; 1891 Colo. LEXIS 158

January, 1891 [January Term]

Context =

PRIOR HISTORY: [***1]

Error to District Court of El Paso County.

THIS is an agreed case, submitted for decision without suit under chapter 24 of the code. The section permitting the submission reads as follows:

"Parties to a question in difference which might be the subject of a civil action may, without action, agree upon a case containing the facts upon which the controversy depends, and present a submission of the same to any court which would have jurisdiction if an action had been brought, but it must appear by affidavit that the controversy is real and the proceedings in good faith to determine the rights of the parties. The court shall thereupon hear and determine the case, and render the judgment thereon as if an action were depending." Sec. 278, Code 1887.

The present controversy has reference to an attempted increase by the city of Colorado Springs of its water supply, such increase becoming necessary on account of the growth of the city; the city being about to purchase from the owners of water-rights for agriculture such rights, to the end that the water may be diverted to the use of the city. The plaintiff, a citizen and tax-payer of the city, and an owner of a water-right for [***2] irrigation purposes upon the Fountain creek hereinafter mentioned, seeks to restrain the city authorities from its contemplated action.

The agreed statement of facts is as follows:

"1. That the defendant is a municipal corporation, being a city of the second class of this state, and has and maintains a system of water-works for the purpose of furnishing, and through which it furnishes, its inhabitants with water.

"2. That the plaintiff is a citizen and tax-payer of the city of Colorado Springs, and an owner of a water-right for irrigation purposes upon the Fountain creek hereinafter mentioned that is prior in right to any appropriation of water made by the defendant, and which is impaired by the defendant's appropriations of water.

"3. That heretofore, in the year 1878, defendant constructed a pipe line and reservoir and supplied and still supplies them with water from Ruxton creek, above the town of Manitou, and that in the year 1889, to supply the increased wants of its inhabitants, defendant greatly enlarged the capacity of said pipe line, reservoir and water-works system, and to supply them now requires about million gallons of water daily, and exceeding the flow [***3] of water in said Ruxton creek; that the waters of the Ruxton and the Fountain creek flow together in the town of Manitou, and that the waters of said creeks at their junction are naturally of about equal volume. That

said Ruxton creek is about five miles in length and is fed and formed by a number of streams coming together above the place of intake of defendant's pipe line, all of which is substantially shown by the map herewith filed.

"4. That defendant has, for the purpose os supplying its said water-works, the first priority of water-rights upon said Ruxton creek, but that there are upon the Fountain creek, below the point where said Ruxton creek and Fountain creeks flow together, a great number of water-rights for irrigation and ranch purposes, prior to defendant's right upon said Ruxton creek, sufficient to take all the waters of Fountain creek after receiving the waters of Ruxton creek.

"5. That defendant takes and will continue to take, for its use, substantially all of the waters of Ruxton creek, so that no waters of Ruxton creek will reach the Fountain creek.

"6. That, in addition to the said pipe line, said defendant is the owner of a certain ditch or canal, known [***4] as the El Paso County canal, which takes water directly from the said Fountain creek for the use of its inhabitants.

"7. That defendant requires both the said pipe line and the said ditch to furnish the necessary supply of water for the use of its inhabitants.

"8. That the water taken from Ruxton creek aforesaid through defendant's pipe line is continuously used by its inhabitants, through its hudrants, for culinary, drinking, general household purposes, sprinkling lawns and streets, in business houses, livery-stables, etc., while the water taken through said ditch or canal is used by defendant to irrigate lawns, parks, trees upon its streets, small gardens, truck patches, etc., continuously from April to October of each year.

"9. That the defendant's said ditch was by the district court of El Paso county in the year 1882, in the adjudication of the priorities of water-rights of water district No. 10, adjudicated to be No. 32, and said original pipe line was then in like manner adjudicated to be No. 1 on Ruxton creek, and that there are thirty-one appropriations of water upon said Fountain creek that are prior to the defendant's said ditch, which are of capacities sufficient [***5] in times of scarcity to take all of the waters of said creek for agricultural purposes; so that in order that defendant have the use of water when it needs it, it must to a great extent interfere with said appropriations that are prior to its ditch and pipe lines, and including the said water-rights to plaintiff.

"10. That the defendant has continuously, including the months from April to October of each year, since the year 1871 to the present year, taken from the waters of said Fountain creek, through its said El Paso County Canal, water to the capacity of said canal, and also has taken continuously through its said original pipe line of the water of said Ruxton creek continuously since the year 1878, waters to the full capacity of said original pipe line, claiming it had a right so to do, and though the plaintiff and other prior appropriators of waters of said Fountain creek have been, to a greater or less degree, for and during each of said periods, injuriously affected thereby, they have failed to object thereto and to assert any prior rights of appropriation he or they had to the water so taken by the defendant, yet said persons, including the plaintiff, now claim damages [***6] therefor of the defendant, and the full amount of their respective original appropriations, without diminution of the amounts so taken

and appropriated by the defendant, which defendant will pay to them unless enjoined by this court.

"11. That many of the persons holding priorities upon said Fountain creek over the defendant, and who are injuriously affected by defendant's said appropriation of water, do not take, and never have taken, through their respective canals or ditches, water to the amount decreed to them in and by the decree aforesaid, because either that their said ditches are not of sufficient capacity to carry such decreed appropriation, or that sufficient water has not been contained in the said creek to supply the amounts so decreed, or that such person has not had under cultivation sufficient land to receive such decreed amount of water; yet, nevertheless, such persons demand of the defendant damages upon the full decreed amount of their respective appropriations, and, unless restrained by this honorable court, the defendant will settle their damages upon such basis.

"12. That the defendant has been negotiating for and is about to purchase some of the water-rights [***7] for agricultural irrigation purposes that are prior to the defendant's ditch and pipe line, with the view of taking the water belonging to such prior water-rights through its said ditch and pipe line for the use of its inhabitants.

"13. That defendant is about to negotiate for such of said water-rights as are prior to its pipe line and its ditch, under and pursuant to subdivision 73 of section 3312 of the General Statutes, upon the basis that such priorities as it so settles for, either by consent or condemnation, deprives such prior appropriator of all his right, title, claim and priority in and to the waters of said Fountain creek, and by such settlement defendant will pay to such prior appropriators sums of money greatly in excess of what it would pay by settling with such prior appropriators, upon the basis that by such settlement or condemnation the said rights remain intact, subject only to diminution to the extent of defendant's uses."

So what is this about?

Plaintiff prays that defendant be enjoined from purchasing water-rights from said Fountain creek, etc., and for general relief. The court below upon a final hearing denied the relief sought by the plaintiff and entered judgment accordingly.

COUNSEL: [***8]

Mr. T. A. McMORRIS, for plaintiff in error.

Mr. WILLIAM HARRISON, for defendant in error.

JUDGES: Before MR. JUSTICE HAYT.

OPINIONBY: HAYT

OPINION: [*66] [**315] MR. JUSTICE HAYT delivered the opinion of the court.

The points upon which a decision is asked as given upon the oral argument may be stated as follows:

1. Are the rights of a junior appropriator of water from a tributary stream subject to the rights of a prior appropriator from the main stream below?

2. Can the priority of a farmer to the use of water for agricultural purposes be transferred by sale to a city for city purposes so that it may succeed to the rights of the original appropriator?

how is this related?

3. To the extent the use made by the city is purely for [*67] domestic purposes, has it the right, without compensation, to take waters theretofore appropriated for agricultural purposes?

That an affirmative answer must be given to the first of the above questions seems obvious. A negative answer would wipe out the doctrine of priorities upon which our elaborate system is based -- a system generally recognized as among the best yet devised, and upon which vast property rights have been built.

The fundamental principle [***9] of this system is that priority in point of time gives superiority of right among appropriators for like beneficial purposes. To now say that an appropriator from the main stream is subject to subsequent appropriation from its tributaries would be the overthrow of the entire doctrine. All large streams are dependent upon tributaries for a supply of water. To cut off the water from such tributaries would be to destroy the capcity of the stream to the injury of those below. It would result in ruinous and useless expenditures of money in a race bwtween rival claimants in the extension of ditches towards the source of water supply, and reward success at the expense of the rights of prior appropriators.

But counsel say: "The waters of the Ruxton lose their identity upon reaching the Fountain. For all purposes to the appropriator, below the point of confluence, Ruxton creek does not exist; it cannot be identified. That being so, how can it be said by the appropriator upon the Fountain creek that the appropriator upon Ruxton creek has taken his water?" It is shown by the stipulation that Ruxton creek is fed and formed by a number of streams coming together above the place of intake [***10] of defendant's pipe line. Now, if plaintiff in error be correct, and the appropriator of water from a stream be held to have no claim upon the water of the tributaries of that stream, then defendant's water supply is liable to be cut off by settlers above at any time -- a conclusion so manifestly unjust that it must be discarded. It is not a question of identity, as [*68] counsel seem to suppose, but one of supply. It is of no consequence to the appropriator below whether the water supplied to him comes from Ruxton creek or from some other tributary to the Fountain; this is entirely immaterial so long as his supply is adequate. When it is lessened by junior appropriators to his injury, he has cause to complain, no matter whether the diminution results from such appropriators taking the water direct from the Fountain, or from some of its tributaries before it reaches the main stream.

not well defined

need new data structure

2. Upon the next proposition plaintiff in error insists that a water-right cannot [**316] be transferred by sale separate from the land. The question thus raised is one of first impression in this court. Its importance is apparent. In Fuller v. Swan River Mining Co., 12 Colo. 12, [***11] a nearer approach was made to its consideration than in any other decided case. It was there held that one who has the right by appropriation to divert the waters of a stream may change the place of diversion and also the place of use. This disposes of plaintiff's contention that the water is only appropriated for a particular tract of land and that the appropriation will not hold for any other; for although the decision is based upon diversion for mining purposes, no reason is perceived why the rule in reference to appropriations for agricultural uses should not be the same, the requirement in all cases being that the water diverted from the stream shall be applied to a beneficial use.

after reviewing the authorities the court said: "It seems to be well

settled by the these decisions that a prior appropriator of water from a stream may change the point of diversion and the place of use without affecting his right of priority, and all the cases reviewed, except the case of Davis v. Gale, 32 Cal. 27, makes the right to make such change dependent upon the condition that the change shall not injuriously affect others. We think that the rule announced in Kidd v. Laird, 15 [***12] Cal. 162, 'that, in the absence of injurious consequences to others, any change which the party chooses to make is legal and proper,' is the only rule [*69] which under the rights of the prior appropriator can be fully exercised, and his rights, and the rights of all other persons fully protected. The right to change, so limited, includes the point of diversion, and place and character of use."

The rule as thus stated seems to be fair to all parties concerned. If A. is the owner of one hundred and sixty acres of land with a water-right for only eighty acres, it may be of great benefit to him to change the place of use as the soil upon a portion of the tract becomes exhausted or impoverished by the raising of crops. To deny the right to change the place of use under such circumstances would result in injury to the prior appropriator with no corresponding benefit to others. The wisdom of the rule in Fuller v. The Swan River Company is apparent when applied in such a case. And no reason is perceived why, if the place of use may be changed to a tract adjoining the one in connection with which the priority came into existence, it may not as well be changed to a piece of [***13] land at a greater distance. The principle permitting the first change to be made being established, the exercise of the right cannot be made to depend upon the locus of the use, provided the rights of others are not injuriously affected by the change. The authority for changing the place of use from one part of a quarter section of land to another place upon the same quarter section will permit the purchase of land elsewhere and utilizing the water in its cultivation. Thus if the owner of land near Ruxton creek with a water-right therefor may purchase land further away from the source of water supply, say at Colorado Springs, and utilize his appropriation for such land, in turn he may sell and convey this land with such water-rights as he may have therefor. And there is nothing to prevent the said city from purchasing both and thereafter changing the place of use the same as any other appropriator. But why force the city to buy the land if it only needs the water?

An examination of the case in 12 Colo. will show the conclusion [*70] there announced to be well supported upin principle and authority. And it being thereby established that the place of use may be changed, [***14] it logically follows that the right to the use of the water for irrigation is a right not so inseparately connected with the land that it may not be separated therefrom. The right has been treated and held as a property right in numerous cases. In Kidd v. Laird, 15 Cal. 161, it is said: "The court has never departed from the doctrine that running water, so long as it continues to flow in its natural course, is not and cannot be made the subject of private ownership. A right may be acquired to its use which will be regarded and protected as property, but it has been distinctly declared in such cases that the right carries with it no specific property in the water itself." Mr Gould in his work on water-rights, at section 234 says, "The right to water acquired by priority is the subject of property and may be sold and conveyed. * * *"

"The exclusive right to divert and use the water of a stream, as well as the ditch or other structure through which the diversion is effected, may be transferred and conveyed like other property or rights analogous to property." Pomeroy on Riparian Rights, par. 58.

The authorities seem to concur in the conclusion that the priority to the use [***15] of water is a property right. To limit its transfer as contended by appellee would in many instances destroy much of its value. It may happen that the soil for which the original appropriation was made has been washed away and lost to the owner, as the result of a freshet or otherwise. To say under such circumstances that he could not sell the water-right to be used upon other land would be to deprive him of all benefits from such right. We grant that the water itself is the property of the public; its use, however, is subject to appropriation, and in this case it is conceded that the owner has the paramount right to such use. In our opinion this right may be transferred by sale so long as the rights of others, as in this case, are not injuriously affected thereby. If the priority [*71] to the use of water for agricultural purposes is a right of property, then the right to sell it is as essential and sacred as the right to possess and use. Blackstone says: "The third absolute right inherent in every Englishman is that of property, which consists in the free use, enjoyment and disposal of all his acquisitions without any control or diminution save only by the laws of the [***16] land." Blackstone, book 1, p. 138.

What difference can it make to others whether the owner of the priority in this case uses it upon his own land or sells it to others to be used [**317] upon other lands? There is no claim of waste occurring between the present points of diversion and the place where the city is to take the water. Where a material waste results from the change, a new feature is introduced which need not be considered here. In chapter 5 of Angell on Water-courses, a number of instances are cited where at common law water-rights were declared to be the subject of sale, and although with us such rights are acquired by appropriation rather than by grant or prescription, as at common law, this certainly cannot affect the right of alienation. In Hurd v. Curtis, 7 Met. 94, several owners of mill privileges had apportioned the water among themselves by a written agreement. By the terms of this instrument one W., the owner of a fulling-mill, was entitled to a certain portion of the water for the use of his mill "or for other machinery requiring equal power," and it was held that the water-right was not inseparably connected with the building or site at which [***17] the water was then used, but that it might be used elsewhere.

In De Witt v. Harvey et al., 4 Gray, 486, a deed had been given of land bordering on a canal supplying mills, "with the privilege of crossing to and from and around the same, and of erecting and using tenter bars in some convenient place near the same, with the privilege also of drawing water from said canal at all times when it may be done without injury to the said mills, sufficient for the purpose of a fulling-mill and shearing machine, but for no other [*72] purposes whatever." And it was held that the right to use the water for a fulling-mill and shearing machine is not made apparent to the land grant, and also that such right was not extinguished by the dam being subsequently taken down by the owners of water-power at that spot and rebuilt in such a manner as to overflow the land granted by the deed; the court being of opinion that the rights of water were not appurtenant to the particular parcel of land granted, but that the owner might use the water at any place or in any manner so long as the rights of others were not thereby impaired. When, therefore, the land became submerged, it was held that the [***18] right of the owner to use the water at any other mill, or upon any other parcel of land situated on the same dam, should be sustained.

There is no controversy in the present case in reference to the mode and manner in which the right to the water may be conveyed, the contention extending further back, the claim being that the right

cannot be conveyed at all, except with the land. The claim is not well founded. As we have seen, the right is the subject of property and may be transferred accordingly, the sole limitation being that the rights of others shall not be injuriously affected by such transfer.

3. Has the city the right to take the water without compensation? This right is claimed under section 6 of article 16 of our constitution. The section relied upon and the preceding section read as follows:

"Sec. 5. The water of every natural stream not heretofore appropriated, within the state of Colorado, is hereby declared to be the property of the public, and the same is dedicated to the use of the people of the state, subject to appropriation as hereinafter provided.

"Sec. 6. The right to divert the unappropriated waters of any natural stream to beneficial [***19] uses shall never be denied.

"Priority of appropriation shall give the better right as between those using the water for the same purpose; but [*73] when the waters of any natural stream are not sufficient for the service of all those desiring the use of the same, those using the water for domestic purposes shall have the preference over those claiming for any other purpose, and those using the water for agricultural purposes shall have preference over those using the same for manufacturing purposes."

As the rights desired by the city accrued prior to the adoption of these constitutional provisions, a well-understood rule of construction, applicable alike to constitutions and statutes, exempts this case from the operation of the constitution in this respect. That instrument operates prospectively only, unless a contrary intention clearly appears from the words employed. Cooley's Const. Limitations, secs. 62, 63.No such intention appears in the provision quoted; in fact the use of the words "not heretofore appropriated," in section 5, and "unappropriated waters," in section 6, clearly indicate an intention to limit the application of these provisions to the future. If, [***20] as urged by plaintiff in error, these provisions were intended to confer upon cities, towns or individuals the right to take without compensation, for domestic use, water appropriated for agrcultural and other purposes before its adoption, they would fall under the ban of the fourteenth amendment to the federal constitution, which provides that no person shall be "deprived of life, liberty or property without due process of law." As we have already seen, a priority to the use of water is a property right.

The construction contended for would also bring the provisions quoted from the state constitution in conflict with several other provisions of that instrument, notably section 3 of the Bill of Rights, in which it is declared, "That all persons have certain rights, among which may be reckoned that of acquiring, possessing and protecting property;" and section 15, which provides that "private property shall not be taken or damaged for public or private use without just compensation;" and section 25, which contains the same [*74] language as that just quoted from the national constitution. And for this reason it should be rejected, it being equally open to a construction that [***21] will at once harmonize and make effective the entire provisions of the instrument in relation to the subject. Our conclusion, therefore, is that the constitutional provisions relied upon were not intended to affect, and do not affect, prior vested rights, but that all owners of such rights are entitled to compensation therefor before the same can be taken or injuriously affected. This is in accordance with the express terms of the statute under which the city is attempting to acquire [**318] a supply of water, as the same was enacted at the

first session of the legislature convened after the adoption of the constitution.

"They shall have the right and privilege of taking water in sufficient quantity, for the purpose hereinbefore mentioned, from any stream, creek, gulch or spring in the state; provided, that if the taking of water in such quantity shall materially interfere with or impair the vested rights of any person or persons or corporation heretofore acquired, residing upon such creek, gulch or stream, or doing any milling or manufacturing business thereon, they shall first obtain the consent of such person or persons or corporation, or acquire the right of domain, [***22] by condemnation, as prescribed by the constitution and laws upon the subject, and make full compensation or satisfaction for all the damages thereby occasioned to such person or persons or corporation." Sec. 73, Gen. Stat. 1883, p. 974.

The statute is instructive as a contemporaneous legislative interpretation of the constitution, aside from the argument to be based upon the fact of the city being purely a creature of statute, and can therefore only exercise the powers conferred in the manner provided by the legislative department.

From anything that we have predicated upon the fact that the water-rights desired by the city antedate the adoption of our constitution, we are not to be understood as intimating that, if the contrary had been the fact, the [*75] rule requiring compensation to be made when such rights are taken for a higher use would be different. The determination of this question is not involved in this case.

The right of a tax-payer to bring an action of this nature has not been raised or considered; for, accepting the agreement of counsel, that he may do so, we are of the opinion, for the reasons given, that the facts relied upon do not constitute a cause [***23] of action. The judgment of the district court denying relief must therefore be affirmed.

Affirmed.

Still don't totally get

Read 9/27

TITLE 17 - COPYRIGHTS
CHAPTER 1 - SUBJECT MATTER AND SCOPE OF COPYRIGHT

§ 102. Subject matter of copyright: In general

(a) Copyright protection subsists, in accordance with this title, in original works of authorship fixed in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. Works of authorship include the following categories:

- **(1)** literary works;
- **(2)** musical works, including any accompanying words;
- **(3)** dramatic works, including any accompanying music;
- **(4)** pantomimes and choreographic works;
- **(5)** pictorial, graphic, and sculptural works;
- **(6)** motion pictures and other audiovisual works;
- **(7)** sound recordings; and
- **(8)** architectural works.

(b) In no case does copyright protection for an original work of authorship extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work.

(Pub. L. 94–553, title I, § 101, Oct. 19, 1976, 90 Stat. 2544; Pub. L. 101–650, title VII, § 703, Dec. 1, 1990, 104 Stat. 5133.)

Historical and Revision Notes

house report no. 94–1476

Original Works of Authorship. The two fundamental criteria of copyright protection—originality and fixation in tangible form are restated in the first sentence of this cornerstone provision. The phrase "original works of authorship," which is purposely left undefined, is intended to incorporate without change the standard of originality established by the courts under the present copyright statute. This standard does not include requirements of novelty, ingenuity, or esthetic merit, and there is no intention to enlarge the standard of copyright protection to require them.

In using the phrase "original works of authorship," rather than "all the writings of an author" now in section 4 of the statute [section 4 of former title 17], the committee's purpose is to avoid exhausting the constitutional power of Congress to legislate in this field, and to eliminate the uncertainties arising from the latter phrase. Since the present statutory language is substantially the same as the empowering language of the Constitution [Const. Art. I, § 8, cl. 8], a recurring question has been whether the statutory and the constitutional provisions are coextensive. If so, the courts would be faced with the alternative of holding copyrightable something that Congress clearly did not intend to protect, or of holding constitutionally incapable of copyright something that Congress might one day want to protect. To avoid these equally undesirable results, the courts have indicated that "all the writings of an author" under the present statute is narrower in scope than the "writings" of "authors" referred to in the Constitution. The bill avoids this dilemma by using a different phrase—"original works of authorship"—in characterizing the general subject matter of statutory copyright protection.

The history of copyright law has been one of gradual expansion in the types of works accorded protection, and the subject matter affected by this expansion has fallen into two general categories. In the first, scientific discoveries and technological developments have made possible new forms of creative expression that never existed before. In some of these cases the new expressive forms—electronic music, filmstrips, and computer programs, for example—could be regarded as an extension of copyrightable subject matter Congress had already intended to protect, and were thus considered copyrightable from the outset without the need of new legislation. In other cases, such as photographs, sound recordings, and motion pictures, statutory enactment was deemed necessary to give them full recognition as copyrightable works.

Authors are continually finding new ways of expressing themselves, but it is impossible to foresee the forms that these new expressive methods will take. The bill does not intend either to freeze the scope of copyrightable subject matter at the present stage of communications technology or to allow unlimited expansion into areas completely outside the

present congressional intent. Section 102 implies neither that that subject matter is unlimited nor that new forms of expression within that general area of subject matter would necessarily be unprotected.

The historic expansion of copyright has also applied to forms of expression which, although in existence for generations or centuries, have only gradually come to be recognized as creative and worthy of protection. The first copyright statute in this country, enacted in 1790, designated only "maps, charts, and books"; major forms of expression such as music, drama, and works of art achieved specific statutory recognition only in later enactments. Although the coverage of the present statute is very broad, and would be broadened further by the explicit recognition of all forms of choreography, there are unquestionably other areas of existing subject matter that this bill does not propose to protect but that future Congresses may want to.

Fixation in Tangible Form. As a basic condition of copyright protection, the bill perpetuates the existing requirement that a work be fixed in a "tangible medium of expression," and adds that this medium may be one "now known or later developed," and that the fixation is sufficient if the work "can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." This broad language is intended to avoid the artificial and largely unjustifiable distinctions, derived from cases such as White-Smith Publishing Co. v. Apollo Co., 209 U.S. 1 (1908) [28 S.Ct. 319, 52 L.Ed. 655], under which statutory copyrightability in certain cases has been made to depend upon the form or medium in which the work is fixed. Under the bill it makes no difference what the form, manner, or medium of fixation may be—whether it is in words, numbers, notes, sounds, pictures, or any other graphic or symbolic indicia, whether embodied in a physical object in written, printed, photographic, sculptural, punched, magnetic, or any other stable form, and whether it is capable of perception directly or by means of any machine or device "now known or later developed."

Under the bill, the concept of fixation is important since it not only determines whether the provisions of the statute apply to a work, but it also represents the dividing line between common law and statutory protection. As will be noted in more detail in connection with section 301, an unfixed work of authorship, such as an improvisation or an unrecorded choreographic work, performance, or broadcast, would continue to be subject to protection under State common law or statute, but would not be eligible for Federal statutory protection under section 102.

The bill seeks to resolve, through the definition of "fixation" in section 101, the status of live broadcasts—sports, news coverage, live performances of music, etc.—that are reaching the public in unfixed form but that are simultaneously being recorded. When a football game is being covered by four television cameras, with a director guiding the activities of the four cameramen and choosing which of their electronic images are sent out to the public and in what order, there is little doubt that what the cameramen and the director are doing constitutes "authorship." The further question to be considered is whether there has been a fixation. If the images and sounds to be broadcast are first recorded (on a video tape, film, etc.) and then transmitted, the recorded work would be considered a "motion picture" subject to statutory protection against unauthorized reproduction or retransmission of the broadcast. If the program content is transmitted live to the public while being recorded at the same time, the case would be treated the same; the copyright owner would not be forced to rely on common law rather than statutory rights in proceeding against an infringing user of the live broadcast.

Thus, assuming it is copyrightable—as a "motion picture" or "sound recording," for example—the content of a live transmission should be regarded as fixed and should be accorded statutory protection if it is being recorded simultaneously with its transmission. On the other hand, the definition of "fixation" would exclude from the concept purely evanescent or transient reproductions such as those projected briefly on a screen, shown electronically on a television or other cathode ray tube, or captured momentarily in the "memory" of a computer.

Under the first sentence of the definition of "fixed" in section 101, a work would be considered "fixed in a tangible medium of expression" if there has been an authorized embodiment in a copy or phonorecord and if that embodiment "is sufficiently permanent or stable" to permit the work "to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration." The second sentence makes clear that, in the case of "a work consisting of sounds, images, or both, that are being transmitted," the work is regarded as "fixed" if a fixation is being made at the same time as the transmission.

Under this definition "copies" and "phonorecords" together will comprise all of the material objects in which copyrightable works are capable of being fixed. The definitions of these terms in section 101, together with their usage in section 102 and throughout the bill, reflect a fundamental distinction between the "original work" which is the product of "authorship" and the multitude of material objects in which it can be embodied. Thus, in the sense of the bill, a "book" is not a work of authorship, but is a particular kind of "copy." Instead, the author may write a "literary work," which in turn can be embodied in a wide range of "copies" and "phonorecords," including books, periodicals, computer punch cards, microfilm, tape recordings, and so forth. It is possible to have an "original work of authorship" without having a "copy" or "phonorecord" embodying it, and it is also possible to have a "copy" or "phonorecord" embodying something that does not qualify as an "original work of authorship." The two essential elements—original work and tangible object—must merge through fixation in order to produce subject matter copyrightable under the statute.

Categories of Copyrightable Works. The second sentence of section 102 lists seven broad categories which the concept of "works of authorship" is said to "include". The use of the word "include," as defined in section 101, makes clear

that the listing is "illustrative and not limitative," and that the seven categories do not necessarily exhaust the scope of "original works of authorship" that the bill is intended to protect. Rather, the list sets out the general area of copyrightable subject matter, but with sufficient flexibility to free the courts from rigid or outmoded concepts of the scope of particular categories. The items are also overlapping in the sense that a work falling within one class may encompass works coming within some or all of the other categories. In the aggregate, the list covers all classes of works now specified in section 5 of title 17 [section 5 of former title 17]; in addition, it specifically enumerates "pantomimes and choreographic works".

Of the seven items listed, four are defined in section 101. The three undefined categories—"musical works," "dramatic works," and "pantomimes and choreographic works"—have fairly settled meanings. There is no need, for example, to specify the copyrightability of electronic or concrete music in the statute since the form of a work would no longer be of any importance, nor is it necessary to specify that "choreographic works" do not include social dance steps and simple routines.

The four items defined in section 101 are "literary works," "pictorial, graphic, and sculptural works," "motion pictures and audiovisual works", and "sound recordings". In each of these cases, definitions are needed not only because the meaning of the term itself is unsettled but also because the distinction between "work" and "material object" requires clarification. The term "literary works" does not connote any criterion of literary merit or qualitative value: it includes catalogs, directories, and similar factual, reference, or instructional works and compilations of data. It also includes computer data bases, and computer programs to the extent that they incorporate authorship in the programmer's expression of original ideas, as distinguished from the ideas themselves.

Correspondingly, the definition of "pictorial, graphic, and sculptural works" carries with it no implied criterion of artistic taste, aesthetic value, or intrinsic quality. The term is intended to comprise not only "works of art" in the traditional sense but also works of graphic art and illustration, art reproductions, plans and drawings, photographs and reproductions of them, maps, charts, globes, and other cartographic works, works of these kinds intended for use in advertising and commerce, and works of "applied art." There is no intention whatever to narrow the scope of the subject matter now characterized in section 5 (k) [section 5(k) of former title 17] as "prints or labels used for articles of merchandise." However, since this terminology suggests the material object in which a work is embodied rather than the work itself, the bill does not mention this category separately.

In accordance with the Supreme Court's decision in Mazer v. Stein, 347 U.S. 201 (1954) [74 S.Ct. 460, 98 L. Ed. 630, rehearing denied 74 S.Ct. 637, 347 U.S. 949, 98 L.Ed. 1096], works of "applied art" encompass all original pictorial, graphic, and sculptural works that are intended to be or have been embodied in useful articles, regardless of factors such as mass production, commercial exploitation, and the potential availability of design patent protection. The scope of exclusive rights in these works is given special treatment in section 113, to be discussed below.

The Committee has added language to the definition of "pictorial, graphic, and sculptural works" in an effort to make clearer the distinction between works of applied art protectable under the bill and industrial designs not subject to copyright protection. The declaration that "pictorial, graphic, and sculptural works" include "works of artistic craftsmanship insofar as their form but not their mechanical or utilitarian aspects are concerned" is classic language; it is drawn from Copyright Office regulations promulgated in the 1940's and expressly endorsed by the Supreme Court in the Mazer case.

The second part of the amendment states that "the design of a useful article * * * shall be considered a pictorial, graphic, or sculptural work only if, and only to the extent that, such design incorporates pictorial, graphic, or sculptural features that can be identified separately from, and are capable of existing independently of, the utilitarian aspects of the article." A "useful article" is defined as "an article having an intrinsic utilitarian function that is not merely to portray the appearance of the article or to convey information." This part of the amendment is an adaptation of language added to the Copyright Office Regulations in the mid-1950's in an effort to implement the Supreme Court's decision in the Mazer case.

In adopting this amendatory language, the Committee is seeking to draw as clear a line as possible between copyrightable works of applied art and uncopyrighted works of industrial design. A two-dimensional painting, drawing, or graphic work is still capable of being identified as such when it is printed on or applied to utilitarian articles such as textile fabrics, wallpaper, containers, and the like. The same is true when a statue or carving is used to embellish an industrial product or, as in the Mazer case, is incorporated into a product without losing its ability to exist independently as a work of art. On the other hand, although the shape of an industrial product may be aesthetically satisfying and valuable, the Committee's intention is not to offer it copyright protection under the bill. Unless the shape of an automobile, airplane, ladies' dress, food processor, television set, or any other industrial product contains some element that, physically or conceptually, can be identified as separable from the utilitarian aspects of that article, the design would not be copyrighted under the bill. The test of separability and independence from "the utilitarian aspects of the article" does not depend upon the nature of the design—that is, even if the appearance of an article is determined by aesthetic (as opposed to functional) considerations, only elements, if any, which can be identified separately from the useful article as such are copyrightable. And, even if the three-dimensional design contains some such element (for

example, a carving on the back of a chair or a floral relief design on silver flatware), copyright protection would extend only to that element, and would not cover the over-all configuration of the utilitarian article as such.

A special situation is presented by architectural works. An architect's plans and drawings would, of course, be protected by copyright, but the extent to which that protection would extend to the structure depicted would depend on the circumstances. Purely nonfunctional or monumental structures would be subject to full copyright protection under the bill, and the same would be true of artistic sculpture or decorative ornamentation or embellishment added to a structure. On the other hand, where the only elements of shape in an architectural design are conceptually inseparable from the utilitarian aspects of the structure, copyright protection for the design would not be available.

The Committee has considered, but chosen to defer, the possibility of protecting the design of typefaces. A "typeface" can be defined as a set of letters, numbers, or other symbolic characters, whose forms are related by repeating design elements consistently applied in a notational system and are intended to be embodied in articles whose intrinsic utilitarian function is for use in composing text or other cognizable combinations of characters. The Committee does not regard the design of typeface, as thus defined, to be a copyrightable "pictorial, graphic, or sculptural work" within the meaning of this bill and the application of the dividing line in section 101.

Enactment of Public Law 92–140 in 1971 [Pub. L. 92–140, Oct. 15, 1971, 85 Stat. 391, which amended sections 1, 5, 19, 20, 26, and 101 of former title 17, and enacted provisions set out as a note under section 1 of former title 17] marked the first recognition in American copyright law of sound recordings as copyrightable works. As defined in section 101, copyrightable "sound recordings" are original works of authorship comprising an aggregate of musical, spoken, or other sounds that have been fixed in tangible form. The copyrightable work comprises the aggregation of sounds and not the tangible medium of fixation. Thus, "sound recordings" as copyrightable subject matter are distinguished from "phonorecords," the latter being physical objects in which sounds are fixed. They are also distinguished from any copyrighted literary, dramatic, or musical works that may be reproduced on a "phonorecord."

As a class of subject matter, sound recordings are clearly within the scope of the "writings of an author" capable of protection under the Constitution [Const. Art. I, § 8, cl. 8], and the extension of limited statutory protection to them was too long delayed. Aside from cases in which sounds are fixed by some purely mechanical means without originality of any kind, the copyright protection that would prevent the reproduction and distribution of unauthorized phonorecords of sound recordings is clearly justified.

The copyrightable elements in a sound recording will usually, though not always, involve "authorship" both on the part of the performers whose performance is captured and on the part of the record producer responsible for setting up the recording session, capturing and electronically processing the sounds, and compiling and editing them to make the final sound recording. There may, however, be cases where the record producer's contribution is so minimal that the performance is the only copyrightable element in the work, and there may be cases (for example, recordings of birdcalls, sounds of racing cars, et cetera) where only the record producer's contribution is copyrightable.

Sound tracks of motion pictures, long a nebulous area in American copyright law, are specifically included in the definition of "motion pictures," and excluded in the definition of "sound recordings." To be a "motion picture," as defined, requires three elements: (1) a series of images, (2) the capability of showing the images in certain successive order, and (3) an impression of motion when the images are thus shown. Coupled with the basic requirements of original authorship and fixation in tangible form, this definition encompasses a wide range of cinematographic works embodied in films, tapes, video disks, and other media. However, it would not include: (1) unauthorized fixations of live performances or telecasts, (2) live telecasts that are not fixed simultaneously with their transmission, or (3) filmstrips and slide sets which, although consisting of a series of images intended to be shown in succession, are not capable of conveying an impression of motion.

On the other hand, the bill equates audiovisual materials such as filmstrips, slide sets, and sets of transparencies with "motion pictures" rather than with "pictorial, graphic, and sculptural works." Their sequential showing is closer to a "performance" than to a "display," and the definition of "audiovisual works," which applies also to "motion pictures," embraces works consisting of a series of related images that are by their nature, intended for showing by means of projectors or other devices.

Nature of Copyright. Copyright does not preclude others from using the ideas or information revealed by the author's work. It pertains to the literary, musical, graphic, or artistic form in which the author expressed intellectual concepts. Section 102 (b) makes clear that copyright protection does not extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such work.

Some concern has been expressed lest copyright in computer programs should extend protection to the methodology or processes adopted by the programmer, rather than merely to the "writing" expressing his ideas. Section 102 (b) is intended, among other things, to make clear that the expression adopted by the programmer is the copyrightable element in a computer program, and that the actual processes or methods embodied in the program are not within the scope of the copyright law.

Section 102 (b) in no way enlarges or contracts the scope of copyright protection under the present law. Its purpose is to restate, in the context of the new single Federal system of copyright, that the basic dichotomy between expression and idea remains unchanged.

Amendments

1990—Subsec. (a)(8). Pub. L. 101–650 added par. (8).

Effective Date of 1990 Amendment

Amendment by Pub. L. 101–650 applicable to any architectural work created on or after Dec. 1, 1990, and any architectural work, that, on Dec. 1, 1990, is unconstructed and embodied in unpublished plans or drawings, except that protection for such architectural work under this title terminates on Dec. 31, 2002, unless the work is constructed by that date, see section 706 of Pub. L. 101–650, set out as a note under section 101 of this title.

TITLE 17 - COPYRIGHTS
CHAPTER 1 - SUBJECT MATTER AND SCOPE OF COPYRIGHT

§ 106. Exclusive rights in copyrighted works

Subject to sections 107 through 122, the owner of copyright under this title has the exclusive rights to do and to authorize any of the following:

(1) to reproduce the copyrighted work in copies or phonorecords;

(2) to prepare derivative works based upon the copyrighted work;

(3) to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending;

(4) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works, to perform the copyrighted work publicly;

(5) in the case of literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works, including the individual images of a motion picture or other audiovisual work, to display the copyrighted work publicly; and

(6) in the case of sound recordings, to perform the copyrighted work publicly by means of a digital audio transmission.

(Pub. L. 94–553, title I, § 101, Oct. 19, 1976, 90 Stat. 2546; Pub. L. 101–318, § 3(d), July 3, 1990, 104 Stat. 288; Pub. L. 101–650, title VII, § 704(b)(2), Dec. 1, 1990, 104 Stat. 5134; Pub. L. 104–39, § 2, Nov. 1, 1995, 109 Stat. 336; Pub. L. 106–44, § 1(g)(2), Aug. 5, 1999, 113 Stat. 222; Pub. L. 107–273, div. C, title III, § 13210(4)(A), Nov. 2, 2002, 116 Stat. 1909.)

Historical and Revision Notes

house report no. 94–1476

General Scope of Copyright. The five fundamental rights that the bill gives to copyright owners—the exclusive rights of reproduction, adaptation, publication, performance, and display—are stated generally in section 106. These exclusive rights, which comprise the so-called "bundle of rights" that is a copyright, are cumulative and may overlap in some cases. Each of the five enumerated rights may be subdivided indefinitely and, as discussed below in connection with section 201, each subdivision of an exclusive right may be owned and enforced separately.

The approach of the bill is to set forth the copyright owner's exclusive rights in broad terms in section 106, and then to provide various limitations, qualifications, or exemptions in the 12 sections that follow. Thus, everything in section 106 is made "subject to sections 107 through 118", and must be read in conjunction with those provisions.

The exclusive rights accorded to a copyright owner under section 106 are "to do and to authorize" any of the activities specified in the five numbered clauses. Use of the phrase "to authorize" is intended to avoid any questions as to the liability of contributory infringers. For example, a person who lawfully acquires an authorized copy of a motion picture would be an infringer if he or she engages in the business of renting it to others for purposes of unauthorized public performance.

Rights of Reproduction, Adaptation, and Publication. The first three clauses of section 106, which cover all rights under a copyright except those of performance and display, extend to every kind of copyrighted work. The exclusive rights encompassed by these clauses, though closely related, are independent; they can generally be characterized as rights of copying, recording, adaptation, and publishing. A single act of infringement may violate all of these rights at once, as where a publisher reproduces, adapts, and sells copies of a person's copyrighted work as part of a publishing venture. Infringement takes place when any one of the rights is violated: where, for example, a printer reproduces copies without selling them or a retailer sells copies without having anything to do with their reproduction. The references to "copies or phonorecords," although in the plural, are intended here and throughout the bill to include the singular (1 U.S.C. § 1).

Reproduction.—Read together with the relevant definitions in section 101, the right "to reproduce the copyrighted work in copies or phonorecords" means the right to produce a material object in which the work is duplicated, transcribed, imitated, or simulated in a fixed form from which it can be "perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." As under the present law, a copyrighted work would be infringed by reproducing it in whole or in any substantial part, and by duplicating it exactly or by imitation or simulation. Wide departures or variations from the copyrighted work would still be an infringement as long as the author's "expression"

rather than merely the author's "ideas" are taken. An exception to this general principle, applicable to the reproduction of copyrighted sound recordings, is specified in section 114.

"Reproduction" under clause (1) of section 106 is to be distinguished from "display" under clause (5). For a work to be "reproduced," its fixation in tangible form must be "sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration." Thus, the showing of images on a screen or tube would not be a violation of clause (1), although it might come within the scope of clause (5).

Preparation of Derivative Works.—The exclusive right to prepare derivative works, specified separately in clause (2) of section 106, overlaps the exclusive right of reproduction to some extent. It is broader than that right, however, in the sense that reproduction requires fixation in copies or phonorecords, whereas the preparation of a derivative work, such as a ballet, pantomime, or improvised performance, may be an infringement even though nothing is ever fixed in tangible form.

To be an infringement the "derivative work" must be "based upon the copyrighted work," and the definition in section 101 refers to "a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which a work may be recast, transformed, or adapted." Thus, to constitute a violation of section 106 (2), the infringing work must incorporate a portion of the copyrighted work in some form; for example, a detailed commentary on a work or a programmatic musical composition inspired by a novel would not normally constitute infringements under this clause.

Use in Information Storage and Retrieval Systems.—As section 117 declares explicitly, the bill is not intended to alter the present law with respect to the use of copyrighted works in computer systems.

Public Distribution.—Clause (3) of section 106 establishes the exclusive right of publication: The right "to distribute copies or phonorecords of the copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending." Under this provision the copyright owner would have the right to control the first public distribution of an authorized copy or phonorecord of his work, whether by sale, gift, loan, or some rental or lease arrangement. Likewise, any unauthorized public distribution of copies or phonorecords that were unlawfully made would be an infringement. As section 109 makes clear, however, the copyright owner's rights under section 106 (3) cease with respect to a particular copy or phonorecord once he has parted with ownership of it.

Rights of Public Performance and Display. Performing Rights and the "For Profit" Limitation.—The right of public performance under section 106 (4) extends to "literary, musical, dramatic, and choreographic works, pantomimes, and motion pictures and other audiovisual works and sound recordings" and, unlike the equivalent provisions now in effect, is not limited by any "for profit" requirement. The approach of the bill, as in many foreign laws, is first to state the public performance right in broad terms, and then to provide specific exemptions for educational and other nonprofit uses.

This approach is more reasonable than the outright exemption of the 1909 statute. The line between commercial and "nonprofit" organizations is increasingly difficult to draw. Many "non-profit" organizations are highly subsidized and capable of paying royalties, and the widespread public exploitation of copyrighted works by public broadcasters and other noncommercial organizations is likely to grow. In addition to these trends, it is worth noting that performances and displays are continuing to supplant markets for printed copies and that in the future a broad "not for profit" exemption could not only hurt authors but could dry up their incentive to write.

The exclusive right of public performance is expanded to include not only motion pictures, including works recorded on film, video tape, and video disks, but also audiovisual works such as filmstrips and sets of slides. This provision of section 106 (4), which is consistent with the assimilation of motion pictures to audiovisual works throughout the bill, is also related to amendments of the definitions of "display" and "perform" discussed below. The important issue of performing rights in sound recordings is discussed in connection with section 114.

Right of Public Display.—Clause (5) of section 106 represents the first explicit statutory recognition in American copyright law of an exclusive right to show a copyrighted work, or an image of it, to the public. The existence or extent of this right under the present statute is uncertain and subject to challenge. The bill would give the owners of copyright in "literary, musical, dramatic, and choreographic works, pantomimes, and pictorial, graphic, or sculptural works", including the individual images of a motion picture or other audiovisual work, the exclusive right "to display the copyrighted work publicly."

Definitions. Under the definitions of "perform," "display," "publicly," and "transmit" in section 101, the concepts of public performance and public display cover not only the initial rendition or showing, but also any further act by which that rendition or showing is transmitted or communicated to the public. Thus, for example: a singer is performing when he or she sings a song; a broadcasting network is performing when it transmits his or her performance (whether simultaneously or from records); a local broadcaster is performing when it transmits the network broadcast; a cable television system is performing when it retransmits the broadcast to its subscribers; and any individual is performing whenever he or she plays a phonorecord embodying the performance or communicates the performance by turning on a receiving set. Although any act by which the initial performance or display is transmitted, repeated, or made to recur would itself be a "performance" or "display" under the bill, it would not be actionable as an infringement unless

it were done "publicly," as defined in section 101. Certain other performances and displays, in addition to those that are "private," are exempted or given qualified copyright control under sections 107 through 118.

To "perform" a work, under the definition in section 101, includes reading a literary work aloud, singing or playing music, dancing a ballet or other choreographic work, and acting out a dramatic work or pantomime. A performance may be accomplished "either directly or by means of any device or process," including all kinds of equipment for reproducing or amplifying sounds or visual images, any sort of transmitting apparatus, any type of electronic retrieval system, and any other techniques and systems not yet in use or even invented.

The definition of "perform" in relation to "a motion picture or other audiovisual work" is "to show its images in any sequence or to make the sounds accompanying it audible." The showing of portions of a motion picture, filmstrip, or slide set must therefore be sequential to constitute a "performance" rather than a "display", but no particular order need be maintained. The purely aural performance of a motion picture sound track, or of the sound portions of an audiovisual work, would constitute a performance of the "motion picture or other audiovisual work"; but, where some of the sounds have been reproduced separately on phonorecords, a performance from the phonorecord would not constitute performance of the motion picture or audiovisual work.

The corresponding definition of "display" covers any showing of a "copy" of the work, "either directly or by means of a film, slide, television image, or any other device or process." Since "copies" are defined as including the material object "in which the work is first fixed," the right of public display applies to original works of art as well as to reproductions of them. With respect to motion pictures and other audiovisual works, it is a "display" (rather than a "performance") to show their "individual images nonsequentially." In addition to the direct showings of a copy of a work, "display" would include the projection of an image on a screen or other surface by any method, the transmission of an image by electronic or other means, and the showing of an image on a cathode ray tube, or similar viewing apparatus connected with any sort of information storage and retrieval system.

Under clause (1) of the definition of "publicly" in section 101, a performance or display is "public" if it takes place "at a place open to the public or at any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered." One of the principal purposes of the definition was to make clear that, contrary to the decision in Metro-Goldwyn-Mayer Distributing Corp. v. Wyatt, 21 C.O.Bull. 203 (D.Md.1932), performances in "semipublic" places such as clubs, lodges, factories, summer camps, and schools are "public performances" subject to copyright control. The term "a family" in this context would include an individual living alone, so that a gathering confined to the individual's social acquaintances would normally be regarded as private. Routine meetings of businesses and governmental personnel would be excluded because they do not represent the gathering of a "substantial number of persons."

Clause (2) of the definition of "publicly" in section 101 makes clear that the concepts of public performance and public display include not only performances and displays that occur initially in a public place, but also acts that transmit or otherwise communicate a performance or display of the work to the public by means of any device or process. The definition of "transmit"—to communicate a performance or display "by any device or process whereby images or sound are received beyond the place from which they are sent"—is broad enough to include all conceivable forms and combinations of wired or wireless communications media, including but by no means limited to radio and television broadcasting as we know them. Each and every method by which the images or sounds comprising a performance or display are picked up and conveyed is a "transmission," and if the transmission reaches the public in my [any] form, the case comes within the scope of clauses (4) or (5) of section 106.

Under the bill, as under the present law, a performance made available by transmission to the public at large is "public" even though the recipients are not gathered in a single place, and even if there is no proof that any of the potential recipients was operating his receiving apparatus at the time of the transmission. The same principles apply whenever the potential recipients of the transmission represent a limited segment of the public, such as the occupants of hotel rooms or the subscribers of a cable television service. Clause (2) of the definition of "publicly" is applicable "whether the members of the public capable of receiving the performance or display receive it in the same place or in separate places and at the same time or at different times."

Amendments

2002—Pub. L. 107–273 substituted "122" for "121" in introductory provisions.

1999—Pub. L. 106–44 substituted "121" for "120" in introductory provisions.

1995—Par. (6). Pub. L. 104–39 added par. (6).

1990—Pub. L. 101–650 substituted "120" for "119" in introductory provisions.

Pub. L. 101–318 substituted "119" for "118" in introductory provisions.

Effective Date of 1995 Amendment

Amendment by Pub. L. 104–39 effective 3 months after Nov. 1, 1995, see section 6 of Pub. L. 104–39, set out as a note under section 101 of this title.

Effective Date of 1990 Amendments

Amendment by Pub. L. 101–650 applicable to any architectural work created on or after Dec. 1, 1990, and any architectural work, that, on Dec. 1, 1990, is unconstructed and embodied in unpublished plans or drawings, except that protection for such architectural work under this title terminates on Dec. 31, 2002, unless the work is constructed by that date, see section 706 of Pub. L. 101–650, set out as a note under section 101 of this title.

Section 3(e)(3) of Pub. L. 101–318 provided that: "The amendment made by subsection (d) [amending this section] shall be effective as of November 16, 1988."

TITLE 17 - COPYRIGHTS
CHAPTER 1 - SUBJECT MATTER AND SCOPE OF COPYRIGHT

Fair Use

§ 107. Limitations on exclusive rights: Fair use

Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include—

(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;

(2) the nature of the copyrighted work;

(3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and

(4) the effect of the use upon the potential market for or value of the copyrighted work.

The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors.

(Pub. L. 94–553, title I, § 101, Oct. 19, 1976, 90 Stat. 2546; Pub. L. 101–650, title VI, § 607, Dec. 1, 1990, 104 Stat. 5132; Pub. L. 102–492, Oct. 24, 1992, 106 Stat. 3145.)

Historical and Revision Notes

Did this actually written by Congress or Cornell,

house report no. 94–1476

General Background of the Problem. The judicial doctrine of fair use, one of the most important and well-established limitations on the exclusive right of copyright owners, would be given express statutory recognition for the first time in section 107. The claim that a defendant's acts constituted a fair use rather than an infringement has been raised as a defense in innumerable copyright actions over the years, and there is ample case law recognizing the existence of the doctrine and applying it. The examples enumerated at page 24 of the Register's 1961 Report, while by no means exhaustive, give some idea of the sort of activities the courts might regard as fair use under the circumstances: "quotation of excerpts in a review or criticism for purposes of illustration or comment; quotation of short passages in a scholarly or technical work, for illustration or clarification of the author's observations; use in a parody of some of the content of the work parodied; summary of an address or article, with brief quotations, in a news report; reproduction by a library of a portion of a work to replace part of a damaged copy; reproduction by a teacher or student of a small part of a work to illustrate a lesson; reproduction of a work in legislative or judicial proceedings or reports; incidental and fortuitous reproduction, in a newsreel or broadcast, of a work located in the scene of an event being reported."

Although the courts have considered and ruled upon the fair use doctrine over and over again, no real definition of the concept has ever emerged. Indeed, since the doctrine is an equitable rule of reason, no generally applicable definition is possible, and each case raising the question must be decided on its own facts. On the other hand, the courts have evolved a set of criteria which, though in no case definitive or determinative, provide some gauge for balancing the equities. These criteria have been stated in various ways, but essentially they can all be reduced to the four standards which have been adopted in section 107: "(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work."

These criteria are relevant in determining whether the basic doctrine of fair use, as stated in the first sentence of section 107, applies in a particular case: "Notwithstanding the provisions of section 106, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright."

The specific wording of section 107 as it now stands is the result of a process of accretion, resulting from the long controversy over the related problems of fair use and the reproduction (mostly by photocopying) of copyrighted material for educational and scholarly purposes. For example, the reference to fair use "by reproduction in copies or phonorecords or by any other means" is mainly intended to make clear that the doctrine has as much application to

photocopying and taping as to older forms of use; it is not intended to give these kinds of reproduction any special status under the fair use provision or to sanction any reproduction beyond the normal and reasonable limits of fair use. Similarly, the newly-added reference to "multiple copies for classroom use" is a recognition that, under the proper circumstances of fairness, the doctrine can be applied to reproductions of multiple copies for the members of a class.

The Committee has amended the first of the criteria to be considered—"the purpose and character of the use"—to state explicitly that this factor includes a consideration of "whether such use is of a commercial nature or is for non-profit educational purposes." This amendment is not intended to be interpreted as any sort of not-for-profit limitation on educational uses of copyrighted works. It is an express recognition that, as under the present law, the commercial or non-profit character of an activity, while not conclusive with respect to fair use, can and should be weighed along with other factors in fair use decisions.

General Intention Behind the Provision. The statement of the fair use doctrine in section 107 offers some guidance to users in determining when the principles of the doctrine apply. However, the endless variety of situations and combinations of circumstances that can rise in particular cases precludes the formulation of exact rules in the statute. The bill endorses the purpose and general scope of the judicial doctrine of fair use, but there is no disposition to freeze the doctrine in the statute, especially during a period of rapid technological change. Beyond a very broad statutory explanation of what fair use is and some of the criteria applicable to it, the courts must be free to adapt the doctrine to particular situations on a case-by-case basis. Section 107 is intended to restate the present judicial doctrine of fair use, not to change, narrow, or enlarge it in any way.

Intention as to Classroom Reproduction. Although the works and uses to which the doctrine of fair use is applicable are as broad as the copyright law itself, most of the discussion of section 107 has centered around questions of classroom reproduction, particularly photocopying. The arguments on the question are summarized at pp. 30–31 of this Committee's 1967 report (H.R. Rep. No. 83, 90th Cong., 1st Sess.), and have not changed materially in the intervening years.

The Committee also adheres to its earlier conclusion, that "a specific exemption freeing certain reproductions of copyrighted works for educational and scholarly purposes from copyright control is not justified." At the same time the Committee recognizes, as it did in 1967, that there is a "need for greater certainty and protection for teachers." In an effort to meet this need the Committee has not only adopted further amendments to section 107, but has also amended section 504 (c) to provide innocent teachers and other non-profit users of copyrighted material with broad insulation against unwarranted liability for infringement. The latter amendments are discussed below in connection with Chapter 5 of the bill [§ 501 et seq. of this title].

In 1967 the Committee also sought to approach this problem by including, in its report, a very thorough discussion of "the considerations lying behind the four criteria listed in the amended section 107, in the context of typical classroom situations arising today." This discussion appeared on pp. 32–35 of the 1967 report, and with some changes has been retained in the Senate report on S. 22 (S. Rep. No. 94–473, pp. 63–65). The Committee has reviewed this discussion, and considers that it still has value as an analysis of various aspects of the problem.

At the Judiciary Subcommittee hearings in June 1975, Chairman Kastenmeier and other members urged the parties to meet together independently in an effort to achieve a meeting of the minds as to permissible educational uses of copyrighted material. The response to these suggestions was positive, and a number of meetings of three groups, dealing respectively with classroom reproduction of printed material, music, and audio-visual material, were held beginning in September 1975.

In a joint letter to Chairman Kastenmeier, dated March 19, 1976, the representatives of the Ad Hoc Committee of Educational Institutions and Organizations on Copyright Law Revision, and of the Authors League of America, Inc., and the Association of American Publishers, Inc., stated:

You may remember that in our letter of March 8, 1976 we told you that the negotiating teams representing authors and publishers and the Ad Hoc Group had reached tentative agreement on guidelines to insert in the Committee Report covering educational copying from books and periodicals under 107 of H.R. 2223 and S. 22 [this section], and that as part of that tentative agreement each side would accept the amendments to Sections 107 and 504 [this section and section 504 of this title] which were adopted by your Subcommittee on March 3, 1976.

We are now happy to tell you that the agreement has been approved by the principals and we enclose a copy herewith. We had originally intended to translate the agreement into language suitable for inclusion in the legislative report dealing with Section 107 [this section], but we have since been advised by committee staff that this will not be necessary.

As stated above, the agreement refers only to copying from books and periodicals, and it is not intended to apply to musical or audiovisual works.

The full text of the agreement is as follows:

Agreement on Guidelines for Classroom Copying in Not-For-Profit Educational Institutions

with respect to books and periodicals

The purpose of the following guidelines is to state the minimum and not the maximum standards of educational fair use under 107 of H.R. 2223 [this section]. The parties agree that the conditions determining the extent of permissible copying for educational purposes may change in the future; that certain types of copying permitted under these guidelines may not be permissible in the future; and conversely that in the future other types of copying not permitted under these guidelines may be permissible under revised guidelines.

Moreover, the following statement of guidelines is not intended to limit the types of copying permitted under the standards of fair use under judicial decision and which are stated in Section 107 of the Copyright Revision Bill [this section]. There may be instances in which copying which does not fall within the guidelines stated below may nonetheless be permitted under the criteria of fair use.

guidelines

I. Single Copying for Teachers

A single copy may be made of any of the following by or for a teacher at his or her individual request for his or her scholarly research or use in teaching or preparation to teach a class:

A. A chapter from a book;

B. An article from a periodical or newspaper;

C. A short story, short essay or short poem, whether or not from a collective work;

D. A chart, graph, diagram, drawing, cartoon or picture from a book, periodical, or newspaper;

II. Multiple Copies for Classroom Use

Multiple copies (not to exceed in any event more than one copy per pupil in a course) may be made by or for the teacher giving the course for classroom use or discussion; provided that:

A. The copying meets the tests of brevity and spontaneity as defined below; and,

B. Meets the cumulative effect test as defined below; and

C. Each copy includes a notice of copyright.

Definitions

Brevity

(i) Poetry: (a) A complete poem if less than 250 words and if printed on not more than two pages or, (b) from a longer poem, an excerpt of not more than 250 words.

(ii) Prose: (a) Either a complete article, story or essay of less than 2,500 words, or (b) an excerpt from any prose work of not more than 1,000 words or 10% of the work, whichever is less, but in any event a minimum of 500 words.

[Each of the numerical limits stated in "i" and "ii" above may be expanded to permit the completion of an unfinished line of a poem or of an unfinished prose paragraph.]

(iii) Illustration: One chart, graph, diagram, drawing, cartoon or picture per book or per periodical issue.

(iv) "Special" works: Certain works in poetry, prose or in "poetic prose" which often combine language with illustrations and which are intended sometimes for children and at other times for a more general audience fall short of 2,500 words in their entirety. Paragraph "ii" above notwithstanding such "special works" may not be reproduced in their entirety; however, an excerpt comprising not more than two of the published pages of such special work and containing not more than 10% of the words found in the text thereof, may be reproduced.

Spontaneity

(i) The copying is at the instance and inspiration of the individual teacher, and

(ii) The inspiration and decision to use the work and the moment of its use for maximum teaching effectiveness are so close in time that it would be unreasonable to expect a timely reply to a request for permission.

Cumulative Effect

(i) The copying of the material is for only one course in the school in which the copies are made.

not MIT x.

(ii) Not more than one short poem, article, story, essay or two excerpts may be copied from the same author, nor more than three from the same collective work or periodical volume during one class term.

(iii) There shall not be more than nine instances of such multiple copying for one course during one class term.

[The limitations stated in "ii" and "iii" above shall not apply to current news periodicals and newspapers and current news sections of other periodicals.]

kinda arbitrary

III. Prohibitions as to I and II Above

Notwithstanding any of the above, the following shall be prohibited:

(A) Copying shall not be used to create or to replace or substitute for anthologies, compilations or collective works. Such replacement or substitution may occur whether copies of various works or excerpts therefrom are accumulated or reproduced and used separately.

(B) There shall be no copying of or from works intended to be "consumable" in the course of study or of teaching. These include workbooks, exercises, standardized tests and test booklets and answer sheets and like consumable material.

(C) Copying shall not:

must pay for those

(a) substitute for the purchase of books, publishers' reprints or periodicals;

(b) be directed by higher authority;

(c) be repeated with respect to the same item by the same teacher from term to term.

but that is the point!

(D) No charge shall be made to the student beyond the actual cost of the photocopying.

Agreed March 19, 1976.

Ad Hoc Committee on Copyright Law Revision:

By Sheldon Elliott Steinbach.

Author-Publisher Group:

Authors League of America:

By Irwin Karp, Counsel.

Association of American Publishers, Inc.:

By Alexander C. Hoffman.

Chairman, Copyright Committee.

In a joint letter dated April 30, 1976, representatives of the Music Publishers' Association of the United States, Inc., the National Music Publishers' Association, Inc., the Music Teachers National Association, the Music Educators National Conference, the National Association of Schools of Music, and the Ad Hoc Committee on Copyright Law Revision, wrote to Chairman Kastenmeier as follows:

During the hearings on H.R. 2223 in June 1975, you and several of your subcommittee members suggested that concerned groups should work together in developing guidelines which would be helpful to clarify Section 107 of the bill [this section].

Representatives of music educators and music publishers delayed their meetings until guidelines had been developed relative to books and periodicals. Shortly after that work was completed and those guidelines were forwarded to your subcommittee, representatives of the undersigned music organizations met together with representatives of the Ad Hoc Committee on Copyright Law Revision to draft guidelines relative to music.

We are very pleased to inform you that the discussions thus have been fruitful on the guidelines which have been developed. Since private music teachers are an important factor in music education, due consideration has been given to the concerns of that group.

We trust that this will be helpful in the report on the bill to clarify Fair Use as it applies to music.

The text of the guidelines accompanying this letter is as follows:

guidelines for educational uses of music

The purpose of the following guidelines is to state the minimum and not the maximum standards of educational fair use under 107 of H.R. 2223 [this section]. The parties agree that the conditions determining the extent of permissible copying for educational purposes may change in the future; that certain types of copying permitted under these guidelines may not be permissible in the future, and conversely that in the future other types of copying not permitted under these guidelines may be permissible under revised guidelines.

Moreover, the following statement of guidelines is not intended to limit the types of copying permitted under the standards of fair use under judicial decision and which are stated in Section 107 of the Copyright Revision Bill [this section]. There may be instances in which copying which does not fall within the guidelines stated below may nonetheless be permitted under the criteria of fair use.

A. Permissible Uses

1. Emergency copying to replace purchased copies which for any reason are not available for an imminent performance provided purchased replacement copies shall be substituted in due course.

2. (a) For academic purposes other than performance, multiple copies of excerpts of works may be made, provided that the excerpts do not comprise a part of the whole which would constitute a performable unit such as a section, movement or aria, but in no case more than 10% of the whole work. The number of copies shall not exceed one copy per pupil.

(b) For academic purposes other than performance, a single copy of an entire performable unit (section, movement, aria, etc.) that is, (1) confirmed by the copyright proprietor to be out of print or (2) unavailable except in a larger work, may be made by or for a teacher solely for the purpose of his or her scholarly research or in preparation to teach a class.

3. Printed copies which have been purchased may be edited or simplified provided that the fundamental character of the work is not distorted or the lyrics, if any, altered or lyrics added if none exist.

4. A single copy of recordings of performances by students may be made for evaluation or rehearsal purposes and may be retained by the educational institution or individual teacher.

5. A single copy of a sound recording (such as a tape, disc or cassette) of copyrighted music may be made from sound recordings owned by an educational institution or an individual teacher for the purpose of constructing aural exercises or examinations and may be retained by the educational institution or individual teacher. (This pertains only to the copyright of the music itself and not to any copyright which may exist in the sound recording.)

B. Prohibitions

1. Copying to create or replace or substitute for anthologies, compilations or collective works.

2. Copying of or from works intended to be "consumable" in the course of study or of teaching such as workbooks, exercises, standardized tests and answer sheets and like material.

3. Copying for the purpose of performance, except as in A(1) above.

4. Copying for the purpose of substituting for the purchase of music, except as in A(1) and A(2) above.

5. Copying without inclusion of the copyright notice which appears on the printed copy.

The problem of off-the-air taping for nonprofit classroom use of copyrighted audiovisual works incorporated in radio and television broadcasts has proved to be difficult to resolve. The Committee believes that the fair use doctrine has some limited application in this area, but it appears that the development of detailed guidelines will require a more thorough exploration than has so far been possible of the needs and problems of a number of different interests affected, and of the various legal problems presented. Nothing in section 107 or elsewhere in the bill is intended to change or prejudge the law on the point. On the other hand, the Committee is sensitive to the importance of the problem, and urges the representatives of the various interests, if possible under the leadership of the Register of Copyrights, to continue their discussions actively and in a constructive spirit. If it would be helpful to a solution, the Committee is receptive to undertaking further consideration of the problem in a future Congress.

The Committee appreciates and commends the efforts and the cooperative and reasonable spirit of the parties who achieved the agreed guidelines on books and periodicals and on music. Representatives of the American Association of University Professors and of the Association of American Law Schools have written to the Committee strongly criticizing the guidelines, particularly with respect to multiple copying, as being too restrictive with respect to classroom situations at the university and graduate level. However, the Committee notes that the Ad Hoc group did include representatives of higher education, that the stated "purpose of the * * * guidelines is to state the minimum and not the maximum standards of educational fair use" and that the agreement acknowledges "there may be instances in which copying which does not fall within the guidelines * * * may nonetheless be permitted under the criteria of fair use."

The Committee believes the guidelines are a reasonable interpretation of the minimum standards of fair use. Teachers will know that copying within the guidelines is fair use. Thus, the guidelines serve the purpose of fulfilling the need for greater certainty and protection for teachers. The Committee expresses the hope that if there are areas where standards other than these guidelines may be appropriate, the parties will continue their efforts to provide additional specific guidelines in the same spirit of good will and give and take that has marked the discussion of this subject in recent months.

Reproduction and Uses for Other Purposes. The concentrated attention given the fair use provision in the context of classroom teaching activities should not obscure its application in other areas. It must be emphasized again that the

same general standards of fair use are applicable to all kinds of uses of copyrighted material, although the relative weight to be given them will differ from case to case.

The fair use doctrine would be relevant to the use of excerpts from copyrighted works in educational broadcasting activities not exempted under section 110 (2) or 112, and not covered by the licensing provisions of section 118. In these cases the factors to be weighed in applying the criteria of this section would include whether the performers, producers, directors, and others responsible for the broadcast were paid, the size and nature of the audience, the size and number of excerpts taken and, in the case of recordings made for broadcast, the number of copies reproduced and the extent of their reuse or exchange. The availability of the fair use doctrine to educational broadcasters would be narrowly circumscribed in the case of motion pictures and other audiovisual works, but under appropriate circumstances it could apply to the nonsequential showing of an individual still or slide, or to the performance of a short excerpt from a motion picture for criticism or comment.

Another special instance illustrating the application of the fair use doctrine pertains to the making of copies or phonorecords of works in the special forms needed for the use of blind persons. These special forms, such as copies in Braille and phonorecords of oral readings (talking books), are not usually made by the publishers for commercial distribution. For the most part, such copies and phonorecords are made by the Library of Congress' Division for the Blind and Physically Handicapped with permission obtained from the copyright owners, and are circulated to blind persons through regional libraries covering the nation. In addition, such copies and phonorecords are made locally by individual volunteers for the use of blind persons in their communities, and the Library of Congress conducts a program for training such volunteers. While the making of multiple copies or phonorecords of a work for general circulation requires the permission of the copyright owner, a problem addressed in section 710 of the bill, the making of a single copy or phonorecord by an individual as a free service for blind persons would properly be considered a fair use under section 107.

Or to each blind copy by a book — Theat DVD case

A problem of particular urgency is that of preserving for posterity prints of motion pictures made before 1942. Aside from the deplorable fact that in a great many cases the only existing copy of a film has been deliberately destroyed, those that remain are in immediate danger of disintegration; they were printed on film stock with a nitrate base that will inevitably decompose in time. The efforts of the Library of Congress, the American Film Institute, and other organizations to rescue and preserve this irreplaceable contribution to our cultural life are to be applauded, and the making of duplicate copies for purposes of archival preservation certainly falls within the scope of "fair use."

When a copyrighted work contains unfair, inaccurate, or derogatory information concerning an individual or institution, the individual or institution may copy and reproduce such parts of the work as are necessary to permit understandable comment on the statements made in the work.

The Committee has considered the question of publication, in Congressional hearings and documents, of copyrighted material. Where the length of the work or excerpt published and the number of copies authorized are reasonable under the circumstances, and the work itself is directly relevant to a matter of legitimate legislative concern, the Committee believes that the publication would constitute fair use.

During the consideration of the revision bill in the 94th Congress it was proposed that independent newsletters, as distinguished from house organs and publicity or advertising publications, be given separate treatment. It is argued that newsletters are particularly vulnerable to mass photocopying, and that most newsletters have fairly modest circulations. Whether the copying of portions of a newsletter is an act of infringement or a fair use will necessarily turn on the facts of the individual case. However, as a general principle, it seems clear that the scope of the fair use doctrine should be considerably narrower in the case of newsletters than in that of either mass-circulation periodicals or scientific journals. The commercial nature of the user is a significant factor in such cases: Copying by a profit-making user of even a small portion of a newsletter may have a significant impact on the commercial market for the work.

The Committee has examined the use of excerpts from copyrighted works in the art work of calligraphers. The committee believes that a single copy reproduction of an excerpt from a copyrighted work by a calligrapher for a single client does not represent an infringement of copyright. Likewise, a single reproduction of excerpts from a copyrighted work by a student calligrapher or teacher in a learning situation would be a fair use of the copyrighted work.

Should make academic journals free

↓

needs further study what will replace it

The Register of Copyrights has recommended that the committee report describe the relationship between this section and the provisions of section 108 relating to reproduction by libraries and archives. The doctrine of fair use applies to library photocopying, and nothing contained in section 108 "in any way affects the right of fair use." No provision of section 108 is intended to take away any rights existing under the fair use doctrine. To the contrary, section 108 authorizes certain photocopying practices which may not qualify as a fair use.

The criteria of fair use are necessarily set forth in general terms. In the application of the criteria of fair use to specific photocopying practices of libraries, it is the intent of this legislation to provide an appropriate balancing of the rights of creators, and the needs of users.

Amendments

1992—Pub. L. 102–492 inserted at end "The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors."

1990—Pub. L. 101–650 substituted "sections 106 and 106A" for "section 106" in introductory provisions.

Effective Date of 1990 Amendment

Amendment by Pub. L. 101–650 effective 6 months after Dec. 1, 1990, see section 610 of Pub. L. 101–650, set out as an Effective Date note under section 106A of this title.

interesting to actually read the law after all this thinking about it

U.S. Supreme Court

BAKER v. SELDEN, 101 U.S. 99 (1879)

101 U.S. 99 101 U.S. 99

BAKER
v.
SELDEN.

October Term, 1879

APPEAL from the Circuit Court of the United States for the Southern District of Ohio.

The facts are stated in the opinion of the court.

Mr. Alphonso Taft and Mr. H. P. Lloyd for the appellant.

Mr. C. W. Moulton and Mr. M. I. Southard for the appellee.

MR. JUSTICE BRADLEY delivered the opinion of the court.

Charles Selden, the testator of the complainant in this case, in the year 1859 took the requisite steps for obtaining the copyright [101 U.S. 99, 100] of a book, entitled 'Selden's Condensed Ledger, or Book-keeping Simplified,' the object of which was to exhibit and explain a peculiar system of book-keeping. In 1860 and 1861, he took the copyright of several other books, containing additions to and improvements upon the said system. The bill of complaint was filed against the defendant, Baker, for an alleged infringement of these copyrights. The latter, in his answer, denied that Selden was the author or designer of the books, and denied the infringement charged, and contends on the argument that the matter alleged to be infringed is not a lawful subject of copyright.

The parties went into proofs, and the various books of the complainant, as well as those sold and used by the defendant, were exhibited before the examiner, and witnesses were examined to both sides. A decree was rendered for the complainant, and the defendant appealed.

The book or series of books of which the complainant claims the copyright consists of an introductory essay explaining the system of book- keeping referred to, to which are annexed certain forms or banks, consisting of ruled lines, and headings, illustrating the system and showing how it is to be used and carried out in practice. This system effects the same results as book-keeping by double entry; but, by a peculiar arrangement of columns and headings, presents the entire operation of a day, a week, or a month, on a single page, or on two pages facing each other, in an account-book. The defendant uses a similar plan so far as results are concerned; but makes a different arrangement of the columns, and uses different headings. If the complainant's testator had the exclusive right to the use of the system explained in his book, it would be difficult to contend that the defendant does not infringe it, notwithstanding the difference in his form of arrangement; but if it be assumed that the system is open to public use, it seems to be equally difficult to contend that the books made and sold by the defendant are a violation of the copyright of the complainant's book considered merely as a book explanatory of the system. Where the truths of a science or the methods of an art are the common property of the whole world, any author has the right to express the one, or explain and use the other, in [101 U.S. 99, 101] his own way. As an author, Selden explained the system in a particular way. It may be conceded that Baker makes and uses account-books arranged on substantially the same system; but the proof fails to show that he has violated the copyright of Selden's book, regarding the latter merely as an explanatory work; or that he has infringed Selden's right in any way, unless the latter became entitled to an exclusive right in the system.

The evidence of the complainant is principally directed to the object of showing that Baker uses the same system as that which is explained and illustrated in Selden's books. It becomes important, therefore, to determine whether, in obtaining the copyright of his books, he secured the exclusive right to the use of the system or method of book-keeping which the said books are intended to illustrate and explain. It is contended that he has secured such exclusive right, because no one can use

Very old

this is a form template protected by copyright

I could see that going both ways

the system without using substantially the same ruled lines and headings which he was appended to his books in illustration of it. In other words, it is contended that the ruled lines and headings, given to illustrate the system, are a part of the book, and, as such, are secured by the copyright; and that no one can make or use similar ruled lines and headings, or ruled lines and headings made and arranged on substantially the same system, without violating the copyright. And this is really the question to be decided in this case. Stated in another form, the question is, whether the exclusive property in a system of book-keeping can be claimed, under the law or copyright, by means of a book in which that system is explained? The complainant's bill, and the case made under it, are based on the hypothesis that it can be.

It cannot be pretended, and indeed it is not seriously urged, that the ruled lines of the complainant's account-book can be claimed under any special class of objects, other than books, named in the law of copyright existing in 1859. The law then in force was that of 1831, and specified only books, maps, charts, musical compositions, prints, and engravings. An account-book, consisting of ruled lines and blank columns, cannot be called by any of these names unless by that of a book.

There is no doubt that a work on the subject of book-keeping, [101 U.S. 99, 102] though only explanatory of well-known systems, may be the subject of a copyright; but, then, it is claimed only as a book. Such a book may be explanatory either of old systems, or of an entirely new system; and, considered as a book, as the work of an author, conveying information on the subject of book-keeping, and containing detailed explanations of the art, it may be a very valuable acquisition to the practical knowledge of the community. But there is a clear distinction between the book, as such, and the art which it is intended to illustrate. The mere statement of the proposition is so evident, that it requires hardly any argument to support it. The same distinction may be predicated of every other art as well as that of book-keeping. A treatise on the composition and use of medicines, be they old or new; on the construction and use of ploughs, or watches, or churns; or on the mixture and application of colors for painting or dyeing; or on the mode of drawing lines to produce the effect of perspective,- would be the subject of copyright; but no one would contend that the copyright of the treatise would give the exclusive right to the art or manufacture described therein. The copyright of the book, if not pirated from other works, would be valid without regard to the novelty, or want of novelty, of its subject-matter. The novelty of the art or thing described or explained has nothing to do with the validity of the copyright. To give to the author of the book an exclusive property in the art described therein, when no examination of its novelty has ever been officially made, would be a surprise and a fraud upon the public. That is the province of letters-patent, not of copyright. The claim to an invention or discovery of an art or manufacture must be subjected to the examination of the Patent Office before an exclusive right therein can be obtained; and it can only be secured by a patent from the government.

The difference between the two things, letters-patent and copyright, may be illustrated by reference to the subjects just enumerated. Take the case of medicines. Certain mixtures are found to be of great value in the healing art. If the discoverer writes and publishes a book on the subject (as regular physicians generally do), he gains no exclusive right to the manufacture and sale of the medicine; he gives that to the [101 U.S. 99, 103] public. If he desires to acquire such exclusive right, he must obtain a patent for the mixture as a new art, manufacture, or composition of matter. He may copyright his book, if he pleases; but that only secures to him the exclusive right of printing and publishing his book. So of all other inventions or discoveries.

The copyright of a book on perspective, no matter how many drawings and illustrations it may contain, gives no exclusive right to the modes of drawing described, though they may never have been known or used before. By publishing the book, without getting a patent for the art, the latter is given to the public. The fact that the art described in the book by illustrations of lines and figures which are reproduced in practice in the application of the art, makes no difference. Those illustrations are the mere language employed by the author to convey his ideas more clearly. Had he used words of description instead of diagrams (which merely stand in the place of words), there could not be the slightest doubt that others, applying the art to practical use, might lawfully draw the lines and diagrams which were in the author's mind, and which he thus described by words in his book.

The copyright of a work on mathematical science cannot give to the author an exclusive right to the methods of operation which he propounds, or to the diagrams which he employs to explain them, so as to prevent an engineer from using them whenever occasion requires. The very object of publishing a book on science or the useful arts is to communicate to the world the useful knowledge which it contains. But this object would be frustrated if the knowledge could not be used without incurring the guilt of piracy of the book. And where the art it teaches cannot be used without employing the methods and diagrams used to illustrate the book, or such as are similar to them, such methods and diagrams are to be considered as necessary incidents to the art, and given therewith to the public; not given for the purpose of publication in other works explanatory of the art, but for the purpose of practical application.

Of course, these observations are not intended to apply to ornamental designs, or pictorial illustrations addressed to the taste. Of these it may be said, that their form is their essence, [101 U.S. 99, 104] and their object, the production of pleasure in their contemplation. This is their final end.

(

So does not apply to system

(not creative enough?

They are as much the product of genius and the result of composition, as are the lines of the poet or the historian's period. On the other hand, the teachings of science and the rules and methods of useful art have their final end in application and use; and this application and use are what the public derive from the publication of a book which teaches them. But as embodied and taught in a literary composition or book, their essence consists only in their statement. This alone is what is secured by the copyright. The use by another of the same methods of statement, whether in words or illustrations, in a book published for teaching the art, would undoubtedly be an infringement of the copyright.

Recurring to the case before us, we observe that Charles Selden, by his books, explained and described a peculiar system of book-keeping, and illustrated his method by means of ruled lines and blank columns, with proper headings on a page, or on successive pages. Now, whilst no one has a right to print or publish his book, or any material part thereof, as a book intended to convey instruction in the art, any person may practise and use the art itself which he has described and illustrated therein. The use of the art is a totally different thing from a publication of the book explaining it. The copyright of a book on book-keeping cannot secure the exclusive right to make, sell, and use account-books prepared upon the plan set forth in such book. Whether the art might or might not have been patented, is a question which is not before us. It was not patented, and is open and free to the use of the public. And, of course, in using the art, the ruled lines and headings of accounts must necessarily be used as incident to it.

The plausibility of the claim put forward by the complainant in this case arises from a confusion of ideas produced by the peculiar nature of the art described in the books which have been made the subject of copyright. In describing the art, the illustrations and diagrams employed happen to correspond more closely than usual with the actual work performed by the operator who uses the art. Those illustrations and diagrams consist of ruled lines and headings of accounts; and [101 U.S. 99, 105] it is similar ruled lines and headings of accounts which, in the application of the art, the book-keeper makes with his pen, or the stationer with his press; whilst in most other cases the diagrams and illustrations can only be represented in concrete forms of wood, metal, stone, or some other physical embodiment. But the principle is the same in all. The description of the art in a book, though entitled to the benefit of copyright, lays no foundation for an exclusive claim to the art itself. The object of the one is explanation; the object of the other is use. The former may be secured by copyright. The latter can only be secured, if it can be secured at all, by letters-patent.

The remarks of Mr. Justice Thompson in the Circuit Court in Clayton v. Stone & Hall (2 Paine, 392), in which copyright was claimed in a daily price-current, are apposite and instructive. He says: 'In determining the true construction to be given to the act of Congress, it is proper to look at the Constitution of the United States, to aid us in ascertaining the nature of the property intended to be protected. 'Congress shall have power to promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right to their writings and discoveries.' The act in question was passed in execution of the power here given, and the object, therefore, was the promotion of science; and it would certainly be a pretty extraordinary view of the sciences to consider a daily or weekly publication of the state of the market as falling within any class of them. They are of a more fixed, permanent, and durable character. The term 'science' cannot, with any propriety, by applied to a work of so fluctuating and fugitive a form as that of a newspaper or price-current, the subject-matter of which is daily changing, and is of mere temporary use. Although great praise may be due to the plaintiffs for their industry and enterprise in publishing this paper, yet the law does not contemplate their being rewarded in this way: it must seek patronage and protection from its utility to the public, and not a work of science. The title of the act of Congress is, 'for the encouragement of learning,' and was not intended for the encouragement of mere industry, unconnected with learning and the sciences. . . . We are, accordingly, of opinion that the paper in question is not [101 U.S. 99, 106] a book the copyright to which can be secured under the act of Congress.'

The case of Cobbett v. Woodward (Law Rep. 14 Eq. 407) was a claim to copyright in a catalogue of furniture which the publisher had on sale in his establishment, illustrated with many drawings of furniture and decorations. The defendants, being dealers in the same business, published a similar book, and copied many of the plaintiff's drawings, though it was shown that they had for sale the articles represented thereby.

The court held that these drawings were not subjects of copyright. Lord Romilly, M. R., said: 'This is a mere advertisement for the sale of particular articles which any one might imitate, and any one might advertise for sale. If a man not being a vendor of any of the articles in question were to publish a work for the purpose of informing the public of what was the most convenient species of articles for household furniture, or the most graceful species of decorations for articles of home furniture, what they ought to cost, and where they might be bought, and were to illustrate his work with designs of each article he described,-such a work as this could not be pirated with impunity, and the attempt to do so would be stopped by the injunction of the Court of Chancery; yet if it were done with no such object, but solely for the purpose of advertising particular articles for sale, and promoting the private trade of the publisher by the sale of articles which any other person might sell as well as the first advertiser, and if in fact it contained little more than an illustrated inventory of the contents of a

warehouse, I know of no law which, while it would not prevent the second advertiser from selling the same articles, would prevent him from using the same advertisement; provided he did not in such advertisement by any device suggest that he was selling the works and designs of the first advertiser.'

Another case, that of Page v. Wisden (20 L. T. N. S. 435), which came before Vice-Chancellor Malins in 1869, has some resemblance to the present. There a copyright was claimed in a cricket scoring-shett, and the Vice- Chancellor held that it was not a fit subject for copyright, partly because it was not new, but also because 'to say that a particular [101 U.S. 99, 107] mode of ruling a book constituted an object for a copyright is absurd.'

These cases, if not precisely in point, come near to the matter in hand, and, in our view, corroborate the general proposition which we have laid down.

In Drury v. Ewing (1 Bond, 540), which is much relied on by the complainant, a copyright was claimed in a chart of patterns for cutting dresses and basques for ladies, and coats, jackets, &c., for boys. It is obvious that such designs could only be printed and published for information, and not for use in themselves. Their practical use could only be exemplified in cloth on the tailor's board and under his shears; in other words, by the application of a mechanical operation to the cutting of cloth in certain patterns and forms. Surely the exclusive right to this practical use was not reserved to the publisher by his copyright of the chart. Without undertaking to say whether we should or should not concur in the decision in that case, we think it cannot control the present.

The conclusion to which we have come is, that blank account-books are not the subject of copyright; and that the mere copyright of Selden's book did not confer upon him the exclusive right to make and use account-books, ruled and arranged as designated by him and described and illustrated in said book.

The decree of the Circuit Court must be reversed, and the cause remanded with instructions to dismiss the complainant's bill; and it is

So ordered

U.S. Supreme Court

SONY CORP. v. UNIVERSAL CITY STUDIOS, INC., 464 U.S. 417 (1984)

464 U.S. 417

SONY CORPORATION OF AMERICA ET AL. v. UNIVERSAL CITY STUDIOS, INC., ET AL.

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

No. 81-1687.

Argued January 18, 1983 Reargued October 3, 1983
Decided January 17, 1984

VCR

Petitioner Sony Corp. manufactures home video tape recorders (VTR's), and markets them through retail establishments, some of which are also petitioners. Respondents own the copyrights on some of the television programs that are broadcast on the public airwaves. Respondents brought an action against petitioners in Federal District Court, alleging that VTR consumers had been recording some of respondents' copy-righted works that had been exhibited on commercially sponsored television and thereby infringed respondents' copyrights, and further that petitioners were liable for such copyright infringement because of their marketing of the VTR's. Respondents sought money damages, an equitable accounting of profits, and an injunction against the manufacture and marketing of the VTR's. The District Court denied respondents all relief, holding that noncommercial home use recording of material broadcast over the public airwaves was a fair use of copyrighted works and did not constitute copyright infringement, and that petitioners could not be held liable as contributory infringers even if the home use of a VTR was considered an infringing use. The Court of Appeals reversed, holding petitioners liable for contributory infringement and ordering the District Court to fashion appropriate relief.

Beta max ?

Yes

Held:

The sale of the VTR's to the general public does not constitute contributory infringement of respondents' copyrights. Pp. 428-456.

(a) The protection given to copyrights is wholly statutory, and, in a case like this, in which Congress has not plainly marked the course to be followed by the judiciary, this Court must be circumspect in construing the scope of rights created by a statute that never contemplated such a calculus of interests. Any individual may reproduce a copyrighted work for a "fair use"; the copyright owner does not possess the exclusive right to such a use. Pp. 428-434.

(b) Kalem Co. v. Harper Brothers, 222 U.S. 55 , does not support respondents' novel theory that supplying the "means" to accomplish an infringing activity and encouraging that activity through advertisement are sufficient to establish liability for copyright infringement. This case does not fall in the category of those in which it is manifestly just to [464 U.S. 417, 418] impose vicarious liability because the "contributory" infringer was in a position to control the use of copyrighted works by others and had authorized the use without permission from the copyright owner. Here, the only contact between petitioners and the users of the VTR's occurred at the moment of sale. And there is no precedent for imposing vicarious liability on the theory that petitioners sold the VTR's with constructive knowledge that their customers might use the equipment to make unauthorized copies of copyrighted material. The sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes, or, indeed, is merely capable of substantial noninfringing uses. Pp. 434-442.

(c) The record and the District Court's findings show (1) that there is a significant likelihood that substantial numbers of copyright holders who license their works for broadcast on free television would not object to having their broadcast time-shifted by private viewers (i. e., recorded at a time when the VTR owner cannot view the broadcast so that it can be watched at a later time); and (2) that there is no likelihood that time-shifting would cause nonminimal harm to the potential market for, or the value of, respondents' copyrighted works. The VTR's are therefore capable of substantial noninfringing uses. Private, noncommercial time-shifting in the home satisfies this standard of noninfringing uses both because respondents have no right to prevent other copyright holders from

authorizing such time-shifting for their programs, and because the District Court's findings reveal that even the unauthorized home time-shifting of respondents' programs is legitimate fair use. Pp. 442-456.

659 F.2d 963, reversed.
STEVENS, J., delivered the opinion of the Court in which BURGER, C. J., and BRENNAN, WHITE, and O'CONNOR, JJ., joined. BLACKMUN, J., filed a dissenting opinion in which MARSHALL, POWELL, and REHNQUIST, JJ., joined, post, p. 457.

Dean C. Dunlavey reargued the cause for petitioners. With him on the briefs were Donald E. Sloan and Marshall Rutter.

Stephen A. Kroft reargued the cause for respondents. With him on the brief was Sondra E. Berchin. *

[Footnote *] Briefs of amici curiae urging reversal were filed for the Virginia Citizens' Consumer Council, Inc., et al. by William A. Dobrovir; for the American Library Association by Newton N. Minow; for the Consumer Electronics Group by J. Edward Day; for the Educators Ad Hoc Committee on [464 U.S. 417, 419] Copyright Law by Michael H. Cardozo, August W. Steinhilber, and Gwendolyn H. Gregory; for General Electric Co. et al. by Alfred B. Engelberg, Morton Amster, Jesse Rothstein, and Joel E. Lutzker; for Hitachi, Ltd., et al. by John W. Armagost and Craig B. Jorgensen; for McCann-Erickson, Inc., et al. by John A. Donovan, A. Howard Matz, and David Fleischer; for Minnesota Mining and Manufacturing Co. et al. by Sidney A. Diamond and Grier Curran Raclin; for the National Retail Merchants Association by Peter R. Stern, Theodore S. Steingut, and Robert A. Weiner; for Sanyo Electric, Inc., by Anthony Liebig; for Sears, Roebuck and Co. by Max L. Gillam and Mary E. Woytek; for TDK Electronics Co., Ltd., by Ko-Yung Tung and Adam Yarmolinsky; for Toshiba Corp. et al. by Donald J. Zoeller and Herve Gouraige; for Pfizer Inc. by Steven C. Kany; and for Viare Publishing by Peter F. Marvin.

Briefs of amici curiae urging affirmance were filed for the Association of American Publishers, Inc., et al. by Charles H. Lieb and Jon A. Baumgarten; for the Authors League of America, Inc., by Irwin Karp; for CBS Inc. by Lloyd N. Cutler, Louis R. Cohen, and George Vradenburg III; for Creators and Distributors of Programs by Stuart Robinowitz and Andrew J. Peck; for the International Alliance of Theatrical Stage Employees and Moving Picture Machine Operators of the United States and Canada, AFL-CIO, by Leo Geffner; for the Motion Picture Association of America, Inc., by Richard M. Cooper, Ellen S. Huvelle, and William Nix; for the National Music Publishers' Association, Inc., by Jon A. Baumgarten; for the Recording Industry Association of America, Inc., by James F. Fitzpatrick, Cary H. Sherman, and Ernest S. Meyers; for Volunteer Lawyers for the Arts, Inc., by I. Fred Koenigsberg; and for the Writers Guild of America, West, Inc., et al. by Paul P. Selvin, Jerome B. Lurie, and Paul S. Berger.

Briefs of amici curiae were filed for the State of Missouri et al. by John Ashcroft, Attorney General of Missouri, and by the Attorneys General for their respective States as follows: Charles A. Graddick of Alabama, John Steven Clark of Arkansas, Michael J. Bowers of Georgia, Tany S. Hong of Hawaii, Tyrone C. Fahner of Illinois, Thomas J. Miller of Iowa, William J. Guste, Jr., of Louisiana, William A. Allain of Mississippi, Michael T. Greely of Montana, Rufus L. Edmisten of North Carolina, William J. Brown of Ohio, Jan Eric Cartwright of Oklahoma, Dennis J. Roberts II of Rhode Island, John J. Easton of Vermont, Gerald L. Baliles of Virginia, and Bronson C. La Follette of Wisconsin; and for the Committee on Copyright [464 U.S. 417, 420] and Literary Property of the Association of the Bar of the City of New York by Michael S. Oberman and David H. Marks. [464 U.S. 417, 419]

JUSTICE STEVENS delivered the opinion of the Court.

Petitioners manufacture and sell home video tape recorders. Respondents own the copyrights on some of the television [464 U.S. 417, 420] programs that are broadcast on the public airwaves. Some members of the general public use video tape recorders sold by petitioners to record some of these broadcasts, as well as a large number of other broadcasts. The question presented is whether the sale of petitioners' copying equipment to the general public violates any of the rights conferred upon respondents by the Copyright Act.

Respondents commenced this copyright infringement action against petitioners in the United States District Court for the Central District of California in 1976. Respondents alleged that some individuals had used Betamax video tape recorders (VTR's) to record some of respondents' copyrighted works which had been exhibited on commercially sponsored television and contended that these individuals had thereby infringed respondents' copyrights. Respondents further maintained that petitioners were liable for the copyright infringement allegedly committed by Betamax consumers because of petitioners' marketing of the Betamax VTR's. 1 Respondents sought no relief against any Betamax consumer. Instead, they sought money damages and an equitable accounting of profits from petitioners, as well as an injunction against the manufacture and marketing of Betamax VTR's.

After a lengthy trial, the District Court denied respondents all the relief they sought and entered judgment for petitioners. 480 F. Supp. 429 (1979). The United States Court of Appeals for the Ninth

Circuit reversed the District Court's judgment on respondents' copyright claim, holding petitioners liable for contributory infringement and ordering the District Court to fashion appropriate relief. 659 F.2d 963 [464 U.S. 417, 421] (1981). We granted certiorari, 457 U.S. 1116 (1982); since we had not completed our study of the case last Term, we ordered reargument, 463 U.S. 1226 (1983). We now reverse.

An explanation of our rejection of respondents' unprecedented attempt to impose copyright liability upon the distributors of copying equipment requires a quite detailed recitation of the findings of the District Court. In summary, those findings reveal that the average member of the public uses a VTR principally to record a program he cannot view as it is being televised and then to watch it once at a later time. This practice, known as "time-shifting," enlarges the television viewing audience. For that reason, a significant amount of television programming may be used in this manner without objection from the owners of the copyrights on the programs. For the same reason, even the two respondents in this case, who do assert objections to time-shifting in this litigation, were unable to prove that the practice has impaired the commercial value of their copyrights or has created any likelihood of future harm. Given these findings, there is no basis in the Copyright Act upon which respondents can hold petitioners liable for distributing VTR's to the general public. The Court of Appeals' holding that respondents are entitled to enjoin the distribution of VTR's, to collect royalties on the sale of such equipment, or to obtain other relief, if affirmed, would enlarge the scope of respondents' statutory monopolies to encompass control over an article of commerce that is not the subject of copyright protection. Such an expansion of the copyright privilege is beyond the limits of the grants authorized by Congress.

I

The two respondents in this action, Universal City Studios, Inc., and Walt Disney Productions, produce and hold the copyrights on a substantial number of motion pictures and other audiovisual works. In the current marketplace, they can exploit their rights in these works in a number of ways: [464 U.S. 417, 422] by authorizing theatrical exhibitions, by licensing limited showings on cable and network television, by selling syndication rights for repeated airings on local television stations, and by marketing programs on prerecorded videotapes or videodiscs. Some works are suitable for exploitation through all of these avenues, while the market for other works is more limited.

Petitioner Sony manufactures millions of Betamax video tape recorders and markets these devices through numerous retail establishments, some of which are also petitioners in this action. 2 Sony's Betamax VTR is a mechanism consisting of three basic components: (1) a tuner, which receives electromagnetic signals transmitted over the television band of the public airwaves and separates them into audio and visual signals; (2) a recorder, which records such signals on a magnetic tape; and (3) an adapter, which converts the audio and visual signals on the tape into a composite signal that can be received by a television set.

Several capabilities of the machine are noteworthy. The separate tuner in the Betamax enables it to record a broadcast off one station while the television set is tuned to another channel, permitting the viewer, for example, to watch two simultaneous news broadcasts by watching one "live" and recording the other for later viewing. Tapes may be reused, and programs that have been recorded may be erased either before or after viewing. A timer in the Betamax can be used to activate and deactivate the equipment at predetermined [464 U.S. 417, 423] times, enabling an intended viewer to record programs that are transmitted when he or she is not at home. Thus a person may watch a program at home in the evening even though it was broadcast while the viewer was at work during the afternoon. The Betamax is also equipped with a pause button and a fast-forward control. The pause button, when depressed, deactivates the recorder until it is released, thus enabling a viewer to omit a commercial advertisement from the recording, provided, of course, that the viewer is present when the program is recorded. The fast-forward control enables the viewer of a previously recorded program to run the tape rapidly when a segment he or she does not desire to see is being played back on the television screen.

The respondents and Sony both conducted surveys of the way the Betamax machine was used by several hundred owners during a sample period in 1978. Although there were some differences in the surveys, they both showed that the primary use of the machine for most owners was "time-shifting" - the practice of recording a program to view it once at a later time, and thereafter erasing it. Time-shifting enables viewers to see programs they otherwise would miss because they are not at home, are occupied with other tasks, or are viewing a program on another station at the time of a broadcast that they desire to watch. Both surveys also showed, however, that a substantial number of interviewees had accumulated libraries of tapes. 3 Sony's survey indicated [464 U.S. 417, 424] that over 80% of the interviewees watched at least as much regular television as they had before owning a Betamax. 4 Respondents offered no evidence of decreased television viewing by Betamax owners. 5

Sony introduced considerable evidence describing television programs that could be copied without objection from any copyright holder, with special emphasis on sports, religious, and educational programming. For example, their survey indicated that 7.3% of all Betamax use is to record sports events, and representatives of professional baseball, football, basketball, and hockey testified that they had no objection to the recording of their televised events for home use. 6 [464 U.S. 417, 425]

Respondents offered opinion evidence concerning the future impact of the unrestricted sale of VTR's on the commercial value of their copyrights. The District Court found, however, that they had failed to prove any likelihood of future harm from the use of VTR's for time-shifting. 480 F. Supp., at 469.

The District Court's Decision

The lengthy trial of the case in the District Court concerned the private, home use of VTR's for recording programs broadcast on the public airwaves without charge to the viewer. 7 No issue concerning the transfer of tapes to other persons, the use of home-recorded tapes for public performances, or the copying of programs transmitted on pay or cable television systems was raised. See id., at 432-433, 442.

The District Court concluded that noncommercial home use recording of material broadcast over the public airwaves was a fair use of copyrighted works and did not constitute copyright infringement. It emphasized the fact that the material was broadcast free to the public at large, the noncommercial character of the use, and the private character of the activity conducted entirely within the home. Moreover, the court found that the purpose of this use served the public interest in increasing access to television programming, an interest that "is consistent with the First Amendment policy of providing the fullest possible access to information through the public airwaves. Columbia Broadcasting System, Inc. v. Democratic National Committee, 412 U.S. 94, 102 ." Id., at 454. 8 Even when an entire copyrighted work was recorded, [464 U.S. 417, 426] the District Court regarded the copying as fair use "because there is no accompanying reduction in the market for `plaintiff's original work.'" Ibid.

As an independent ground of decision, the District Court also concluded that Sony could not be held liable as a contributory infringer even if the home use of a VTR was considered an infringing use. The District Court noted that Sony had no direct involvement with any Betamax purchasers who recorded copyrighted works off the air. Sony's advertising was silent on the subject of possible copyright infringement, but its instruction booklet contained the following statement:

"Television programs, films, videotapes and other materials may be copyrighted. Unauthorized recording of such material may be contrary to the provisions of the United States copyright laws." Id., at 436.

The District Court assumed that Sony had constructive knowledge of the probability that the Betamax machine would be used to record copyrighted programs, but found that Sony merely sold a "product capable of a variety of uses, some of them allegedly infringing." Id., at 461. It reasoned:

"Selling a staple article of commerce - e. g., a typewriter, a recorder, a camera, a photocopying machine - technically contributes to any infringing use subsequently made thereof, but this kind of `contribution,' if deemed sufficient as a basis for liability, would expand the theory beyond precedent and arguably beyond judicial management.

.....

"... Commerce would indeed be hampered if manufacturers of staple items were held liable as contributory infringers whenever they `constructively' knew that some purchasers on some occasions would use their product [464 U.S. 417, 427] for a purpose which a court later deemed, as a matter of first impression, to be an infringement." Ibid.

Finally, the District Court discussed the respondents' prayer for injunctive relief, noting that they had asked for an injunction either preventing the future sale of Betamax machines, or requiring that the machines be rendered incapable of recording copyrighted works off the air. The court stated that it had "found no case in which the manufacturers, distributors, retailers and advertisers of the instrument enabling the infringement were sued by the copyright holders," and that the request for relief in this case "is unique." Id., at 465.
It concluded that an injunction was wholly inappropriate because any possible harm to respondents was outweighed by the fact that "the Betamax could still legally be used to record noncopyrighted material or material whose owners consented to the copying. An injunction would deprive the public of the ability to use the Betamax for this noninfringing off-the-air recording." Id., at 468.

The Court of Appeals' Decision

The Court of Appeals reversed the District Court's judgment on respondents' copyright claim. It did not set aside any of the District Court's findings of fact. Rather, it concluded as a matter of law that the home use of a VTR was not a fair use because it was not a "productive use." 9 It therefore held that it was unnecessary for plaintiffs to prove any harm to the potential market for the copyrighted works, but then observed that it seemed clear that the cumulative effect of mass reproduction made possible by VTR's would tend to diminish the potential market for respondents' works. 659 F.2d, at 974. [464 U.S. 417, 428]

On the issue of contributory infringement, the Court of Appeals first rejected the analogy to staple

articles of commerce such as tape recorders or photocopying machines. It noted that such machines "may have substantial benefit for some purposes" and do not "even remotely raise copyright problems." Id., at 975. VTR's, however, are sold "for the primary purpose of reproducing television programming" and "[v]irtually all" such programming is copyrighted material. Ibid. The Court of Appeals concluded, therefore, that VTR's were not suitable for any substantial noninfringing use even if some copyright owners elect not to enforce their rights.

The Court of Appeals also rejected the District Court's reliance on Sony's lack of knowledge that home use constituted infringement. Assuming that the statutory provisions defining the remedies for infringement applied also to the nonstatutory tort of contributory infringement, the court stated that a defendant's good faith would merely reduce his damages liability but would not excuse the infringing conduct. It held that Sony was chargeable with knowledge of the homeowner's infringing activity because the reproduction of copyrighted materials was either "the most conspicuous use" or "the major use" of the Betamax product. Ibid.

On the matter of relief, the Court of Appeals concluded that "statutory damages may be appropriate" and that the District Court should reconsider its determination that an injunction would not be an appropriate remedy; and, referring to "the analogous photocopying area," suggested that a continuing royalty pursuant to a judicially created compulsory license may very well be an acceptable resolution of the relief issue. Id., at 976.

II

Article I, 8, of the Constitution provides:

"The Congress shall have Power . . . To Promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." [464 U.S. 417, 429]

The monopoly privileges that Congress may authorize are neither unlimited nor primarily designed to provide a special private benefit. Rather, the limited grant is a means by which an important public purpose may be achieved. It is intended to motivate the creative activity of authors and inventors by the provision of a special reward, and to allow the public access to the products of their genius after the limited period of exclusive control has expired.

"The copyright law, like the patent statutes, makes reward to the owner a secondary consideration. In Fox Film Corp. v. Doyal, 286 U.S. 123, 127 , Chief Justice Hughes spoke as follows respecting the copyright monopoly granted by Congress, `The sole interest of the United States and the primary object in conferring the monopoly lie in the general benefits derived by the public from the labors of authors.' It is said that reward to the author or artist serves to induce release to the public of the products of his creative genius." United States v. Paramount Pictures, Inc., 334 U.S. 131, 158 (1948).

As the text of the Constitution makes plain, it is Congress that has been assigned the task of defining the scope of the limited monopoly that should be granted to authors or to inventors in order to give the public appropriate access to their work product. Because this task involves a difficult balance between the interests of authors and inventors in the control and exploitation of their writings and discoveries on the one hand, and society's competing interest in the free flow of ideas, information, and commerce on the other hand, our patent and copyright statutes have been amended repeatedly. 10
[464 U.S. 417, 430]
From its beginning, the law of copyright has developed in response to significant changes in technology. 11 Indeed, it was the invention of a new form of copying equipment - the printing press - that gave rise to the original need for copyright protection. 12 Repeatedly, as new developments have [464 U.S. 417, 431] occurred in this country, it has been the Congress that has fashioned the new rules that new technology made necessary. Thus, long before the enactment of the Copyright Act of 1909, 35 Stat. 1075, it was settled that the protection given to copyrights is wholly statutory. Wheaton v. Peters, 8 Pet. 591, 661-662 (1834). The remedies for infringement "are only those prescribed by Congress." Thompson v. Hubbard, 131 U.S. 123, 151 (1889).

The judiciary's reluctance to expand the protections afforded by the copyright without explicit legislative guidance is a recurring theme. See, e. g., Teleprompter Corp. v. Columbia Broadcasting System, Inc., 415 U.S. 394 (1974); Fortnightly Corp. v. United Artists Television, Inc., 392 U.S. 390 (1968); White-Smith Music Publishing Co. v. Apollo Co., 209 U.S. 1 (1908); Williams & Wilkins Co. v. United States, 203 Ct. Cl. 74, 487 F.2d 1345 (1973), aff'd by an equally divided Court, 420 U.S. 376 (1975). Sound policy, as well as history, supports our consistent deference to Congress when major technological innovations alter the market for copyrighted materials. Congress has the constitutional authority and the institutional ability to accommodate fully the varied permutations of competing interests that are inevitably implicated by such new technology.

In a case like this, in which Congress has not plainly marked our course, we must be circumspect in construing the scope of rights created by a legislative enactment which never contemplated such a calculus of interests. In doing so, we are guided by Justice Stewart's exposition of the correct approach to ambiguities in the law of copyright:

"The limited scope of the copyright holder's statutory monopoly, like the limited copyright duration required by the Constitution, reflects a balance of competing claims upon the public interest: Creative work is to be [464 U.S. 417, 432] encouraged and rewarded, but private motivation must ultimately serve the cause of promoting broad public availability of literature, music, and the other arts. The immediate effect of our copyright law is to secure a fair return for an `author's' creative labor. But the ultimate aim is, by this incentive, to stimulate artistic creativity for the general public good. `The sole interest of the United States and the primary object in conferring the monopoly,' this Court has said, `lie in the general benefits derived by the public from the labors of authors.' Fox Film Corp. v. Doyal, 286 U.S. 123, 127 . See Kendall v. Winsor, 21 How. 322, 327-328; Grant v. Raymond, 6 Pet. 218, 241-242. When technological change has rendered its literal terms ambiguous, the Copyright Act must be construed in light of this basic purpose." Twentieth Century Music Corp. v. Aiken, 422 U.S. 151, 156 (1975) (footnotes omitted).

Copyright protection "subsists . . . in original works of authorship fixed in any tangible medium of expression." 17 U.S.C. 102(a) (1982 ed.). This protection has never accorded the copyright owner complete control over all possible uses of his work. 13 Rather, the Copyright Act grants the [464 U.S. 417, 433] copyright holder "exclusive" rights to use and to authorize the use of his work in five qualified ways, including reproduction of the copyrighted work in copies. 106. 14 All reproductions of the work, however, are not within the exclusive domain of the copyright owner; some are in the public domain. Any individual may reproduce a copyrighted work for a "fair use"; the copyright owner does not possess the exclusive right to such a use. Compare 106 with 107.

"Anyone who violates any of the exclusive rights of the copyright owner," that is, anyone who trespasses into his exclusive domain by using or authorizing the use of the copyrighted work in one of the five ways set forth in the statute, "is an infringer of the copyright." 501(a). Conversely, anyone who is authorized by the copyright owner to use the copyrighted work in a way specified in the statute or who makes a fair use of the work is not an infringer of the copyright with respect to such use.

The Copyright Act provides the owner of a copyright with a potent arsenal of remedies against an infringer of his work, including an injunction to restrain the infringer from violating [464 U.S. 417, 434] his rights, the impoundment and destruction of all reproductions of his work made in violation of his rights, a recovery of his actual damages and any additional profits realized by the infringer or a recovery of statutory damages, and attorney's fees. 502-505. 15

The two respondents in this case do not seek relief against the Betamax users who have allegedly infringed their copyrights. Moreover, this is not a class action on behalf of all copyright owners who license their works for television broadcast, and respondents have no right to invoke whatever rights other copyright holders may have to bring infringement actions based on Betamax copying of their works. 16 As was made clear by their own evidence, the copying of the respondents' programs represents a small portion of the total use of VTR's. It is, however, the taping of respondents' own copyrighted programs that provides them with standing to charge Sony with contributory infringement. To prevail, they have the burden of proving that users of the Betamax have infringed their copyrights and that Sony should be held responsible for that infringement.

III

The Copyright Act does not expressly render anyone liable for infringement committed by another. In contrast, the [464 U.S. 417, 435] Patent Act expressly brands anyone who "actively induces infringement of a patent" as an infringer, 35 U.S.C. 271(b), and further imposes liability on certain individuals labeled "contributory" infringers, 271(c). The absence of such express language in the copyright statute does not preclude the imposition of liability for copyright infringements on certain parties who have not themselves engaged in the infringing activity. 17 For vicarious liability is imposed in virtually all areas of the law, and the concept of contributory infringement is merely a species of the broader problem of identifying the circumstances in which it is just to hold one individual accountable for the actions of another.

Such circumstances were plainly present in Kalem Co. v. Harper Brothers, 222 U.S. 55 (1911), the copyright decision of this Court on which respondents place their principal reliance. In Kalem, the Court held that the producer of an unauthorized film dramatization of the copyrighted book Ben Hur was liable for his sale of the motion picture to jobbers, who in turn arranged for the commercial exhibition of the film. Justice Holmes, writing for the Court, explained:

"The defendant not only expected but invoked by advertisement the use of its films for dramatic reproduction [464 U.S. 417, 436] of the story. That was the most conspicuous purpose for which they could be used, and the one for which especially they were made. If the defendant did not contribute to the infringement it is impossible to do so except by taking part in the final act. It is liable on principles recognized in every part of the law." Id., at 62-63.

The use for which the item sold in Kalem had been "especially" made was, of course, to display the performance that had already been recorded upon it. The producer had personally appropriated the copyright owner's protected work and, as the owner of the tangible medium of expression upon which

the protected work was recorded, authorized that use by his sale of the film to jobbers. But that use of the film was not his to authorize: the copyright owner possessed the exclusive right to authorize public performances of his work. Further, the producer personally advertised the unauthorized public performances, dispelling any possible doubt as to the use of the film which he had authorized. Respondents argue that Kalem stands for the proposition that supplying the "means" to accomplish an infringing activity and encouraging that activity through advertisement are sufficient to establish liability for copyright infringement. This argument rests on a gross generalization that cannot withstand scrutiny. The producer in Kalem did not merely provide the "means" to accomplish an infringing activity; the producer supplied the work itself, albeit in a new medium of expression. Sony in the instant case does not supply Betamax consumers with respondents' works; respondents do. Sony supplies a piece of equipment that is generally capable of copying the entire range of programs that may be televised: those that are uncopyrighted, those that are copyrighted but may be copied without objection from the copyright holder, and those that the copyright holder would prefer not to have copied. The Betamax can be used to [464 U.S. 417, 437] make authorized or unauthorized uses of copyrighted works, but the range of its potential use is much broader than the particular infringing use of the film Ben Hur involved in Kalem. Kalem does not support respondents' novel theory of liability.

Justice Holmes stated that the producer had "contributed" to the infringement of the copyright, and the label "contributory infringement" has been applied in a number of lower court copyright cases involving an ongoing relationship between the direct infringer and the contributory infringer at the time the infringing conduct occurred. In such cases, as in other situations in which the imposition of vicarious liability is manifestly just, the "contributory" infringer was in a position to control the use of copyrighted works by others and had authorized the use without permission from the copyright owner. 18 This case, however, plainly does not fall [464 U.S. 417, 438] in that category. The only contact between Sony and the users of the Betamax that is disclosed by this record occurred at the moment of sale. The District Court expressly found that "no employee of Sony, Sonam or DDBI had either direct involvement with the allegedly infringing activity or direct contact with purchasers of Betamax who recorded copyrighted works off-the-air." 480 F. Supp., at 460. And it further found that "there was no evidence that any of the copies made by Griffiths or the other individual witnesses in this suit were influenced or encouraged by [Sony's] advertisements." Ibid. [464 U.S. 417, 439]

If vicarious liability is to be imposed on Sony in this case, it must rest on the fact that it has sold equipment with constructive knowledge of the fact that its customers may use that equipment to make unauthorized copies of copyrighted material. There is no precedent in the law of copyright for the imposition of vicarious liability on such a theory. The closest analogy is provided by the patent law cases to which it is appropriate to refer because of the historic kinship between patent law and copyright law. 19 [464 U.S. 417, 440]

In the Patent Act both the concept of infringement and the concept of contributory infringement are expressly defined by statute. 20 The prohibition against contributory infringement is confined to the knowing sale of a component especially made for use in connection with a particular patent. There is no suggestion in the statute that one patentee may object to the sale of a product that might be used in connection with other patents. Moreover, the Act expressly provides that the sale of a "staple article or commodity of commerce suitable for substantial noninfringing use" is not contributory infringement. 35 U.S.C. 271(c).

When a charge of contributory infringement is predicated entirely on the sale of an article of commerce that is used by the purchaser to infringe a patent, the public interest in access to that article of commerce is necessarily implicated. A [464 U.S. 417, 441] finding of contributory infringement does not, of course, remove the article from the market altogether; it does, however, give the patentee effective control over the sale of that item. Indeed, a finding of contributory infringement is normally the functional equivalent of holding that the disputed article is within the monopoly granted to the patentee. 21

For that reason, in contributory infringement cases arising under the patent laws the Court has always recognized the critical importance of not allowing the patentee to extend his monopoly beyond the limits of his specific grant. These cases deny the patentee any right to control the distribution of unpatented articles unless they are "unsuited for any commercial noninfringing use." Dawson Chemical Co. v. Rohm & Hass Co., 448 U.S. 176, 198 (1980). Unless a commodity "has no use except through practice of the patented method," id., at 199, the patentee has no right to claim that its distribution constitutes contributory infringement. "To form the basis for contributory infringement the item must almost be uniquely suited as a component of the patented invention." P. Rosenberg, Patent Law Fundamentals 17.022. (2d ed. 1982). "[A] sale of an article which though adapted to an infringing use is also adapted to other and lawful uses, is not enough to make the seller a contributory infringer. Such a rule would block the wheels of commerce." Henry v. A. B. Dick Co., 224 U.S. 1, 48 (1912), overruled on other grounds, [464 U.S. 417, 442] Motion Picture Patents Co. v. Universal Film Mfg. Co., 243 U.S. 502, 517 (1917).

We recognize there are substantial differences between the patent and copyright laws. But in both

areas the contributory infringement doctrine is grounded on the recognition that adequate protection of a monopoly may require the courts to look beyond actual duplication of a device or publication to the products or activities that make such duplication possible. The staple article of commerce doctrine must strike a balance between a copyright holder's legitimate demand for effective - not merely symbolic - protection of the statutory monopoly, and the rights of others freely to engage in substantially unrelated areas of commerce. Accordingly, the sale of copying equipment, like the sale of other articles of commerce, does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses.

IV

The question is thus whether the Betamax is capable of commercially significant noninfringing uses. In order to resolve that question, we need not explore all the different potential uses of the machine and determine whether or not they would constitute infringement. Rather, we need only consider whether on the basis of the facts as found by the District Court a significant number of them would be noninfringing. Moreover, in order to resolve this case we need not give precise content to the question of how much use is commercially significant. For one potential use of the Betamax plainly satisfies this standard, however it is understood: private, noncommercial time-shifting in the home. It does so both (A) because respondents have no right to prevent other copyright holders from authorizing it for their programs, and (B) because the District Court's factual findings reveal that even the unauthorized home time-shifting of respondents' programs is legitimate fair use. [464 U.S. 417, 443]

A. Authorized Time-Shifting

Each of the respondents owns a large inventory of valuable copyrights, but in the total spectrum of television programming their combined market share is small. The exact percentage is not specified, but it is well below 10%. 22 If they were to prevail, the outcome of this litigation would have a significant impact on both the producers and the viewers of the remaining 90% of the programming in the Nation. No doubt, many other producers share respondents' concern about the possible consequences of unrestricted copying. Nevertheless the findings of the District Court make it clear that time-shifting may enlarge the total viewing audience and that many producers are willing to allow private time-shifting to continue, at least for an experimental time period. 23

The District Court found:

"Even if it were deemed that home-use recording of copyrighted material constituted infringement, the Betamax could still legally be used to record noncopyrighted material or material whose owners consented to the copying. An injunction would deprive the public of the ability to use the Betamax for this noninfringing off-the-air recording. [464 U.S. 417, 444]

"Defendants introduced considerable testimony at trial about the potential for such copying of sports, religious, educational and other programming. This included testimony from representatives of the Offices of the Commissioners of the National Football, Basketball, Baseball and Hockey Leagues and Associations, the Executive Director of National Religious Broadcasters and various educational communications agencies. Plaintiffs attack the weight of the testimony offered and also contend that an injunction is warranted because infringing uses outweigh noninfringing uses.

"Whatever the future percentage of legal versus illegal home-use recording might be, an injunction which seeks to deprive the public of the very tool or article of commerce capable of some noninfringing use would be an extremely harsh remedy, as well as one unprecedented in copyright law." 480 F. Supp., at 468.

Although the District Court made these statements in the context of considering the propriety of injunctive relief, the statements constitute a finding that the evidence concerning "sports, religious, educational and other programming" was sufficient to establish a significant quantity of broadcasting whose copying is now authorized, and a significant potential for future authorized copying. That finding is amply supported by the record. In addition to the religious and sports officials identified explicitly by the District Court, 24 two items in the record deserve specific mention. [464 U.S. 417, 445]

First is the testimony of John Kenaston, the station manager of Channel 58, an educational station in Los Angeles affiliated with the Public Broadcasting Service. He explained and authenticated the station's published guide to its programs. 25 For each program, the guide tells whether unlimited home taping is authorized, home taping is authorized subject to certain restrictions (such as erasure within seven days), or home taping is not authorized at all. The Spring 1978 edition of the guide described 107 programs. Sixty-two of those programs or 58% authorize some home taping. Twenty-one of them or almost 20% authorize unrestricted home taping. 26

Second is the testimony of Fred Rogers, president of the corporation that produces and owns the copyright on Mister Rogers' Neighborhood. The program is carried by more public television stations than any other program. Its audience numbers over 3,000,000 families a day. He testified that he had absolutely no objection to home taping for noncommercial use and expressed the opinion that it is a

real service to families to be able to record children's programs and to show them at appropriate times. 27 [464 U.S. 417, 446]

If there are millions of owners of VTR's who make copies of televised sports events, religious broadcasts, and educational programs such as Mister Rogers' Neighborhood, and if the proprietors of those programs welcome the practice, the business of supplying the equipment that makes such copying feasible should not be stifled simply because the equipment is used by some individuals to make unauthorized reproductions of respondents' works. The respondents do not represent a class composed of all copyright holders. Yet a finding of contributory infringement would inevitably frustrate the interests of broadcasters in reaching the portion of their audience that is available only through time-shifting.

Of course, the fact that other copyright holders may welcome the practice of time-shifting does not mean that respondents should be deemed to have granted a license to copy their programs. Third-party conduct would be wholly irrelevant in an action for direct infringement of respondents' copyrights. But in an action for contributory infringement against the seller of copying equipment, the copyright holder may not prevail unless the relief that he seeks affects only his programs, or unless he speaks for virtually all copyright holders with an interest in the outcome. In this case, the record makes it perfectly clear that there are many important producers of national and local television programs who find nothing objectionable about the enlargement in the size of the television audience that results from the practice of time-shifting for private home use. 28 The seller of the equipment that expands those producers' audiences cannot be a contributory [464 U.S. 417, 447] infringer if, as is true in this case, it has had no direct involvement with any infringing activity.

B. Unauthorized Time-Shifting

Even unauthorized uses of a copyrighted work are not necessarily infringing. An unlicensed use of the copyright is not an infringement unless it conflicts with one of the specific exclusive rights conferred by the copyright statute. Twentieth Century Music Corp. v. Aiken, 422 U.S., at 154 -155. Moreover, the definition of exclusive rights in 106 of the present Act is prefaced by the words "subject to sections 107 through 118." Those sections describe a variety of uses of copyrighted material that "are not infringements of copyright" "notwithstanding the provisions of section 106." The most pertinent in this case is 107, the legislative endorsement of the doctrine of "fair use." 29 [464 U.S. 417, 448]

That section identifies various factors 30 that enable a court to apply an "equitable rule of reason" analysis to particular claims of infringement. 31 Although not conclusive, the first [464 U.S. 417, 449] factor requires that "the commercial or nonprofit character of an activity" be weighed in any fair use decision. 32 If the Betamax were used to make copies for a commercial or profitmaking purpose, such use would presumptively be unfair. The contrary presumption is appropriate here, however, because the District Court's findings plainly establish that time-shifting for private home use must be characterized as a noncommercial, nonprofit activity. Moreover, when one considers the nature of a televised copyrighted audiovisual work, see 17 U.S.C. 107(2) (1982 ed.), and that time-shifting merely enables a viewer to see such a work which he had been invited to witness in its entirety free of charge, the fact [464 U.S. 417, 450] that the entire work is reproduced, see 107(3), does not have its ordinary effect of militating against a finding of fair use. 33

This is not, however, the end of the inquiry because Congress has also directed us to consider "the effect of the use upon the potential market for or value of the copyrighted work." 107(4). The purpose of copyright is to create incentives for creative effort. Even copying for noncommercial purposes may impair the copyright holder's ability to obtain the rewards that Congress intended him to have. But a use that has no demonstrable effect upon the potential market for, or the value of, the copyrighted work need not be prohibited in order to protect the author's incentive to create. The prohibition of such noncommercial uses would [464 U.S. 417, 451] merely inhibit access to ideas without any countervailing benefit. 34

Thus, although every commercial use of copyrighted material is presumptively an unfair exploitation of the monopoly privilege that belongs to the owner of the copyright, noncommercial uses are a different matter. A challenge to a noncommercial use of a copyrighted work requires proof either that the particular use is harmful, or that if it should become widespread, it would adversely affect the potential market for the copyrighted work. Actual present harm need not be shown; such a requirement would leave the copyright holder with no defense against predictable damage. Nor is it necessary to show with certainty that future harm will result. What is necessary is a showing by a preponderance of the evidence that some meaningful likelihood of future harm exists. If the intended use is for commercial gain, that likelihood may be presumed. But if it is for a noncommercial purpose, the likelihood must be demonstrated.

In this case, respondents failed to carry their burden with regard to home time-shifting. The District Court described respondents' evidence as follows:

"Plaintiffs' experts admitted at several points in the trial that the time-shifting without librarying would result in `not a great deal of harm.' Plaintiffs' greatest concern about time-shifting is with `a

point of important philosophy that transcends even commercial judgment.' They fear that with any Betamax usage, `invisible boundaries' are passed: `the copyright owner has lost control over his program.'" 480 F. Supp., at 467. [464 U.S. 417, 452]

Later in its opinion, the District Court observed:

"Most of plaintiffs' predictions of harm hinge on speculation about audience viewing patterns and ratings, a measurement system which Sidney Sheinberg, MCA's president, calls a `black art' because of the significant level of imprecision involved in the calculations." Id., at 469. 35

There was no need for the District Court to say much about past harm. "Plaintiffs have admitted that no actual harm to their copyrights has occurred to date." Id., at 451.
On the question of potential future harm from time-shifting, the District Court offered a more detailed analysis of the evidence. It rejected respondents' "fear that persons `watching' the original telecast of a program will not be measured in the live audience and the ratings and revenues will decrease," by observing that current measurement technology allows the Betamax audience to be reflected. Id., at 466. 36 It rejected respondents' prediction "that live television [464 U.S. 417, 453] or movie audiences will decrease as more people watch Betamax tapes as an alternative," with the observation that "[t]here is no factual basis for [the underlying] assumption." Ibid. 37 It rejected respondents' "fear that time-shifting will reduce audiences for telecast reruns," and concluded instead that "given current market practices, this should aid plaintiffs rather than harm them." Ibid. 38 And it declared that respondents' suggestion that "theater or film rental exhibition of a program will suffer because of time-shift recording of that program" "lacks merit." Id., at 467. 39 [464 U.S. 417, 454]

After completing that review, the District Court restated its overall conclusion several times, in several different ways. "Harm from time-shifting is speculative and, at best, minimal." Ibid. "The audience benefits from the time-shifting capability have already been discussed. It is not implausible that benefits could also accrue to plaintiffs, broadcasters, and advertisers, as the Betamax makes it possible for more persons to view their broadcasts." Ibid. "No likelihood of harm was shown at trial, and plaintiffs admitted that there had been no actual harm to date." Id., at 468-469. "Testimony at trial suggested that Betamax may require adjustments in marketing strategy, but it did not establish even a likelihood of harm." Id., at 469. "Television production by plaintiffs today is more profitable than it has ever been, and, in five weeks of trial, there was no concrete evidence to suggest that the Betamax will change the studios' financial picture." Ibid.

The District Court's conclusions are buttressed by the fact that to the extent time-shifting expands public access to freely broadcast television programs, it yields societal benefits. In Community Television of Southern California v. Gottfried, 459 U.S. 498, 508 , n. 12 (1983), we acknowledged the public interest in making television broadcasting more available. Concededly, that interest is not unlimited. But it supports an interpretation of the concept of "fair use" that requires the copyright holder to demonstrate some likelihood of harm before he may condemn a private act of time-shifting as a violation of federal law.

When these factors are all weighed in the "equitable rule of reason" balance, we must conclude that this record amply [464 U.S. 417, 455] supports the District Court's conclusion that home time-shifting is fair use. In light of the findings of the District Court regarding the state of the empirical data, it is clear that the Court of Appeals erred in holding that the statute as presently written bars such conduct. 40 [464 U.S. 417, 456]

In summary, the record and findings of the District Court lead us to two conclusions. First, Sony demonstrated a significant likelihood that substantial numbers of copyright holders who license their works for broadcast on free television would not object to having their broadcasts time-shifted by private viewers. And second, respondents failed to demonstrate that time-shifting would cause any likelihood of nonminimal harm to the potential market for, or the value of, their copyrighted works. The Betamax is, therefore, capable of substantial noninfringing uses. Sony's sale of such equipment to the general public does not constitute contributory infringement of respondents' copyrights.

V

"The direction of Art. I is that Congress shall have the power to promote the progress of science and the useful arts. When, as here, the Constitution is permissive, the sign of how far Congress has chosen to go can come only from Congress." Deepsouth Packing Co. v. Laitram Corp., 406 U.S. 518, 530 (1972).

One may search the Copyright Act in vain for any sign that the elected representatives of the millions of people who watch television every day have made it unlawful to copy a program for later viewing at home, or have enacted a flat prohibition against the sale of machines that make such copying possible. It may well be that Congress will take a fresh look at this new technology, just as it so often has examined other innovations in the past. But it is not our job to apply laws that have not yet been written. Applying the copyright statute, as it now reads, to the facts as they have been developed in this case, the judgment of the Court of Appeals must be reversed.

(11)

Alan: Takedown provisions misused in wild
Must actually find + send notice
3rd party does as contractors
So chilling effects.org

Technical tools make diff in practical app. of this

Important in Viacom vs Youtube case

Why diff than Betamax
Such a large % is infringing
So real notice

Specific circumstances
~~them~~ "red flag" provision
L general awareness of infringement

(need to read this stuff closer)

(12)

"Bad facts"

- like we're going to get sued

"Unfortunate emails"

Could have actual knowledge

No obligation to police your site

- Content cos want them to police

Content-id system

Made a 10 min limit

Would hash file + check future uploads

- on DMCA notice

or figure out ahead of time

- Can send YouTube a reference copy

lots of work internally

- no false positives

(13)

bt diff resolutions

Small clips

2 qv

1. Auto takedown

gave copyright holders a choice

— take down

— let us put ads on for ya

↑ 80% picked this object

2. Fair use claims

Content providers loved it

Showed Google wanted to be good citizen

Controversal internally

Slipery slope

Q° What % of YouTube is Copyright

- depends where you sit
- Congress said few
- Alan i Hundreds of people, Million of $

(14)

Does it be a requirement for the next Youtube
So start up barrier

Section 1! 'standard technical measures in industry'
J

(missed)

Trying to work out vol. agreements w/ rights holders
'3 strikes'
now 6 w/ last one vague
Do ya have the role protecting users' rights here?

So much worse globally,
not same safe harbors
much more concern from liability from other countries

(15)

(What group should I choose
I like all the topics - and don't love one - like net neutrality

Cyber security group

What subtopics?

For next week: 1 pg proposal well written

(also who want to work w/ Christina timil

policy

a bit of military

Cyber warfare

inducing defense

- websites
- water plants) diff levels

Vs privacy or other stuff

protecting code

disclosure

(6)

Narrow down ?

military - cyber warfare

Do you release vulnerabilities

Compare them to crypto system

Where should cybersecurity be go

financial

ethical

polity

Presentations

End of next week Super finalized

frame an issue

challenge for admin

framework to

(17)

Privacy

Do not track beyond web browser

What is privacy?

Sensing

What is the real answer?

Anonimity

Lots of ⊕ effects

but lots of cons

Poli: legislative options

or agencies set tech standards

~~Medical Privacy~~ Global

which laws apply to it

Diff approaches

international relations

free flow of info

(18)

Pat: lots to do

Like doctrines

Copyright international

Pat: lots of stuff

look at existing efforts

Survey recent legislation

KR SOPA + PIPA

Why didn't go through

Prof: timly

What to do after

Focus

- SOPA pretty specific

(19)

Cyber security (us)

1. Where invest resources
2. Defence + attack
3. What cyberware fare allowed?

Stuxnet + flare

Pat: Broad

You named 7, pick 1

Lots of stuff written

Need to say where starting

Quality ideas not that high

ideas very large

Sensor on aircraft / UAV

(20)

(I like the proto-SOPA)

Prof: lack of careful scoping

Global Governance

Understand current policy

no more than 2 pg proposal

Prof: Can you articulate a question

6.805 Class 5, Oct. 4: Open Internet

Class 5, Oct. 4, 2012 - Network Neutrality and the End-to-End Internet

6.805: Foundations of Internet Policy - Semester Calendar

Goals

This week we'll be looking at the issues surrounding "network neutrality" and Internet access. The end-to-end model of Internet communication -- long taken as an article of faith -- is increasingly challenged by the growing market concentration and activities of broadband network providers. We'll take a close look at the debate this has spawned over net neutrality and non-discrimination on the Internet.

For our second hour of class, we'll be joined by MIT's own David Clark. Dave is a long-time researcher at CSAIL and one of the early architects of the end-to-end principles. He also one of the more thoughtful people on the technical and policy ramifications of network operator activities. Come armed with good questions!

Finally, we'll spend a significant portion of class finalizing our 2013 Agenda projects and teams.

Team Assignment from last week (due October 1 on Stellar)

Each team should turn in a page saying what issue you plan to investigate, and how you propose to go about it, and cite at least four references you will be using. Express the issue as a specific issue where you will make policy recommendations to the incoming Administration.

pre research

Class Readings for this week

End-to-end principles and their role in Internet policy

- J.H. Saltzer, D.P. Reed and D.D. Clark, "End to End Arguments in System Design", ACM Transactions on Computer Systems 2.4 (1984). Focus on the sections titled Introduction, Other Examples, and Conclusion.
- Vinton G. Cerf, Prepared Statement before the U.S. Senate Committee on Commerce, Science, and Transportation Hearing on "Network Neutrality" (Feb. 7, 2006).

The open Internet or "network neutrality" debate

- Tim Wu, "Net Neutrality FAQ". Wu is credited with coining the term and has been a leading voice for Internet non-discrimination.
- Comments of AT&T Inc., In the Matter of Preserving the Open Internet, FCC GN Docket No. 09-191 (submitted Jan. 14, 2010). Read the Executive Summary (pp. 1-17).
- Federal Communications Commission, Report and Order in the Matter of Preserving the Open

Internet, FCC 10-201 (Dec. 2010).
  - Skim the report (first ~80 pages) but carefully read the proposed rule, in Appendix A at pages 88-89 in the order. This is the law of the land... for now.
  - Read the dissent of Commissioner McDowell, pages 145-152.

Legal issues and the ongoing debate

- Susan Crawford, "Chapter 2: Regulatory Pendulum -- The Long Twilight Struggle", excerpt from the book *Captive Audience* (forthcoming 2013). This is still a work-in-progress and should be not be distributed beyond members of the class.
- Nate Anderson, "US net neutrality rules finalized", Ars Technica (Sept. 22, 2011); Don Jeffrey, "Group Challenges FCC's Open-Internet Rules in Boston Court", Bloomberg Businessweek (Sept. 28, 2011).
- Facetime: "AT&T defends FaceTime decision: 'There is no net neutrality violation'", ArsTechnica (Aug. 22, 2012). (See also, Public Knowledge complaint and AT&T response).

For further enlightenment [purely optional]:

- The ill-fated Google-Verizon proposal, August 2010: Original Goblog post; NY Times story; ZDnet analysis.
- Susan Crawford, "The Communications Crisis in America", 5 Harvard Law & Policy Review 246 (2011).
- Blumenthal, M. S. and D. D. Clark, "Rethinking the Design of the Internet: The End-to-End Arguments vs. the Brave New World", ACM Transactions on Internet Technology 1.1 (2001)
- Barbara von Schewick, *Open Architecture and Innovation* (2010).

In Class Timeline

2:00 - 2:15	Introduction to "Open Internet" topic [ABD]
2:15 - 2:30	Overview of Administrative Procedure, role of federal agencies [DJW]
2:30 - 3:00	Discussion: The net neutrality debate [ABD]
3:00 - 4:00	Guest: David Clark [ABD]
4:00 - 4:15	break
4:15 - 4:55	Agenda 2013 Activity [DJW + all]
4:55 - 5:00	Preview next week's class [DJW/AD]

Individual writing assignment for next week:

Due October 8 on Stellar

It is January 2013. You work as a staffer for the Senate Commerce Committee. As you arrive at work you see (on the ubiquitous TVs scattered throughout your offices) that the DC Circuit Court of Appeals has just vacated the FCC's "open internet" rules. A three-judge panel has ruled that the FCC lacked the statutory authority (claimed under Title I of the Telecom Act) to make the rules in the first place.

Your boss, the Senator who chairs this powerful committee, will control the Senate's consideration of any legislation regarding the FCC and the Internet – including responses to the court's ruling. As she races out of the office for a vote, she shouts over to you:

> *"What's this whole FCC Internet court case thing again? Can you get me a quick memo on it – including what you think we should do next? I'm sure to get asked by the press this afternoon. And remember: I won't read anything more than two pages long!"*

Write a short memo for your boss (you can decide if she's a Republican or Democrat.) It should include a brief summary of the issues in the case, what it means for the internet and consumers, the relative merits of giving the FCC authority to deal with this problem, and a recommendation for what your boss and the committee should do next (or at least what she should say to the press!)

Team preparation for next week

For next week's class, each team should present its plan for doing research, including a problem statement, writing, and schedule for meeting with your mentor. Each team should also present a plan for how they will divide up the work. One person on the team needs to be selected as the report editor, and will have overall responsibility for the final product.

END-TO-END ARGUMENTS IN SYSTEM DESIGN

J.H. Saltzer, D.P. Reed and D.D. Clark*

M.I.T. Laboratory for Computer Science

This paper presents a design principle that helps guide placement of functions among the modules of a distributed computer system. The principle, called the end-to-end argument, suggests that functions placed at low levels of a system may be redundant or of little value when compared with the cost of providing them at that low level. Examples discussed in the paper include bit error recovery, security using encryption, duplicate message suppression, recovery from system crashes, and delivery acknowledgement. Low level mechanisms to support these functions are justified only as performance enhancements.

Introduction

Choosing the proper boundaries between functions is perhaps the primary activity of the computer system designer. Design principles that provide guidance in this choice of function placement are among the most important tools of a system designer. This paper discusses one class of function placement argument that has been used for many years with neither explicit recognition nor much conviction. However, the emergence of the data communication network as a computer system component has sharpened this line of function placement argument by making more apparent the situations in which and reasons why it applies. This paper articulates the argument explicitly, so as to examine its nature and to see how general it really is. The argument appeals to application requirements, and provides a rationale for moving function upward in a layered system, closer to the application that uses the function. We begin by considering the communication network version of the argument.

In a system that includes communications, one usually draws a modular boundary around the communication subsystem and defines a firm interface between it and the rest of the system. When doing so, it becomes apparent that there is a list of functions each of which might be implemented in any of several ways: by the communication subsystem, by its client, as a joint

---

* Authors' addresses: J.H. Saltzer and D.D. Clark, M.I.T. Laboratory for Computer Science, 545 Technology Square, Cambridge, Massachusetts 02139.: D.P. Reed, Software Arts, Inc., 27 Mica Lane, Wellesley, Massachusetts 02181.

This research was supported in part by the Advanced Research Projects Agency of the U.S. Department of Defense and monitored by the Office of Naval Research under contract number N00014-75-C-0661.

Revised version of a paper from the Second International Conference on Distributed Computing Systems, Paris, France, April 8-10, 1981, pp. 509-512.:

Published in ACM Transactions in Computer Systems 2, 4, November, 1984, pages 277-288.

Reprinted in Craig Partridge, editor Innovations in internetworking. Artech House, Norwood, MA, 1988, pages 195-206. ISBN 0-89006-337-0. Also scheduled to be reprinted in Amit Bhargava, editor. Integrated broadband networks. Artech House, Boston, 1991. ISBN 0-89006-483-0.

Scribe/FinalWord source: http://web.mit.edu/Saltzer/www/publications/

venture, or perhaps redundantly, each doing its own version. In reasoning about this choice, the requirements of the application provide the basis for a class of arguments, which go as follows:

> The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the end points of the communication system. Therefore, providing that questioned function as a feature of the communication system itself is not possible. (Sometimes an incomplete version of the function provided by the communication system may be useful as a performance enhancement.)

We call this line of reasoning against low-level function implementation the "end-to-end argument." The following sections examine the end-to-end argument in detail, first with a case study of a typical example in which it is used – the function in question is reliable data transmission – and then by exhibiting the range of functions to which the same argument can be applied. For the case of the data communication system, this range includes encryption, duplicate message detection, message sequencing, guaranteed message delivery, detecting host crashes, and delivery receipts. In a broader context the argument seems to apply to many other functions of a computer operating system, including its file system. Examination of this broader context will be easier if we first consider the more specific data communication context, however.

End-to-end caretaking

Consider the problem of "careful file transfer." A file is stored by a file system, in the disk storage of computer A. Computer A is linked by a data communication network with computer B, which also has a file system and a disk store. The object is to move the file from computer A's storage to computer B's storage without damage, in the face of knowledge that failures can occur at various points along the way. The application program in this case is the file transfer program, part of which runs at host A and part at host B. In order to discuss the possible threats to the file's integrity in this transaction, let us assume that the following specific steps are involved:

1. At host A the file transfer program calls upon the file system to read the file from the disk, where it resides on several tracks, and the file system passes it to the file transfer program in fixed-size blocks chosen to be disk-format independent.
2. Also at host A the file transfer program asks the data communication system to transmit the file using some communication protocol that involves splitting the data into packets. The packet size is typically different from the file block size and the disk track size.
3. The data communication network moves the packets from computer A to computer B.
4. At host B a data communication program removes the packets from the data communication protocol and hands the contained data on to a second part of the file transfer application, the part that operates within host B.
5. At host B, the file transfer program asks the file system to write the received data on the disk of host B.

With this model of the steps involved, the following are some of the threats to the transaction that a careful designer might be concerned about:

1. The file, though originally written correctly onto the disk at host A, if read now may contain incorrect data, perhaps because of hardware faults in the disk storage system.
2. The software of the file system, the file transfer program, or the data communication system might make a mistake in buffering and copying the data of the file, either at host A or host B.
3. The hardware processor or its local memory might have a transient error while doing the buffering and copying, either at host A or host B.
4. The communication system might drop or change the bits in a packet, or lose a packet or deliver a packet more than once.

5. Either of the hosts may crash part way through the transaction after performing an unknown amount (perhaps all) of the transaction.

How would a careful file transfer application then cope with this list of threats? One approach might be to reinforce each of the steps along the way using duplicate copies, timeout and retry, carefully located redundancy for error detection, crash recovery, etc. The goal would be to reduce the probability of each of the individual threats to an acceptably small value. Unfortunately, systematic countering of threat two requires writing correct programs, which task is quite difficult, and not all the programs that must be correct are written by the file transfer application programmer. If we assume further that all these threats are relatively low in probability – low enough that the system allows useful work to be accomplished – brute force countermeasures such as doing everything three times appear uneconomical.

The alternate approach might be called "end-to-end check and retry". Suppose that as an aid to coping with threat number one, stored with each file is a checksum that has sufficient redundancy to reduce the chance of an undetected error in the file to an acceptably negligible value. The application program follows the simple steps above in transferring the file from A to B. Then, as a final additional step, the part of the file transfer application residing in host B reads the transferred file copy back from its disk storage system into its own memory, recalculates the checksum, and sends this value back to host A, where it is compared with the checksum of the original. Only if the two checksums agree does the file transfer application declare the transaction committed. If the comparison fails, something went wrong, and a retry from the beginning might be attempted.

If failures really are fairly rare, this technique will normally work on the first try; occasionally a second or even third try might be required; one would probably consider two or more failures on the same file transfer attempt as indicating that some part of the system is in need of repair.

Now let us consider the usefulness of a common proposal, namely that the communication system provide, internally, a guarantee of reliable data transmission. It might accomplish this guarantee by providing selective redundancy in the form of packet checksums, sequence number checking, and internal retry mechanisms, for example. With sufficient care, the probability of undetected bit errors can be reduced to any desirable level. The question is whether or not this attempt to be helpful on the part of the communication system is useful to the careful file transfer application.

The answer is that threat number four may have been eliminated, but the careful file transfer application must still counter the remaining threats, so it should still provide its own retries based on an end-to-end checksum of the file. And if it does so, the extra effort expended in the communication system to provide a guarantee of reliable data transmission is only reducing the frequency of retries by the file transfer application; it has no effect on inevitability or correctness of the outcome, since correct file transmission is assured by the end-to-end checksum and retry whether or not the data transmission system is especially reliable.

Thus the argument: in order to achieve careful file transfer, the application program that performs the transfer must supply a file-transfer-specific, end-to-end reliability guarantee – in this case, a checksum to detect failures and a retry/commit plan. For the data communication system to go out of its way to be extraordinarily reliable does not reduce the burden on the application program to ensure reliability.

A too-real example

An interesting example of the pitfalls that one can encounter turned up recently at M.I.T.: One network system involving several local networks connected by gateways used a packet checksum on each hop from one gateway to the next, on the assumption that the primary threat to correct communication was corruption of bits during transmission. Application programmers, aware of

this checksum, assumed that the network was providing reliable transmission, without realizing that the transmitted data was unprotected while stored in each gateway. One gateway computer developed a transient error in which while copying data from an input to an output buffer a byte pair was interchanged, with a frequency of about one such interchange in every million bytes passed. Over a period of time many of the source files of an operating system were repeatedly transferred through the defective gateway. Some of these source files were corrupted by byte exchanges, and their owners were forced to the ultimate end-to-end error check: manual comparison with and correction from old listings.

Performance aspects

It would be too simplistic to conclude that the lower levels should play no part in obtaining reliability, however. Consider a network that is somewhat unreliable, dropping one message of each hundred messages sent. The simple strategy outlined above, transmitting the file and then checking to see that the file arrived correctly, would perform more poorly as the length of the file increases. The probability that all packets of a file arrive correctly decreases exponentially with the file length, and thus the expected time to transmit the file grows exponentially with file length. Clearly, some effort at the lower levels to improve network reliability can have a significant effect on application performance. But the key idea here is that the lower levels need not provide "perfect" reliability.

Thus the amount of effort to put into reliability measures within the data communication system is seen to be an engineering tradeoff based on performance, rather than a requirement for correctness. Note that performance has several aspects here. If the communication system is too unreliable, the file transfer application performance will suffer because of frequent retries following failures of its end-to-end checksum. If the communication system is beefed up with internal reliability measures, those measures have a performance cost, too, in the form of bandwidth lost to redundant data and delay added by waiting for internal consistency checks to complete before delivering the data. There is little reason to push in this direction very far, when it is considered that *the end-to-end check of the file transfer application must still be implemented no matter how reliable the communication system becomes*. The "proper" tradeoff requires careful thought; for example one might start by designing the communication system to provide just the reliability that comes with little cost and engineering effort, and then evaluate the residual error level to insure that it is consistent with an acceptable retry frequency at the file transfer level. It is probably not important to strive for a negligible error rate at any point below the application level.

Using performance to justify placing functions in a low-level subsystem must be done carefully. Sometimes, by examining the problem thoroughly, the same or better performance enhancement can be achieved at the high level. Performing a function at a low level may be more efficient, if the function can be performed with a minimum perturbation of the machinery already included in the low-level subsystem, but just the opposite situation can occur – that is, performing the function at the lower level may cost more – for two reasons. First, since the lower level subsystem is common to many applications, those applications that do not need the function will pay for it anyway. Second, the low-level subsystem may not have as much information as the higher levels, so it cannot do the job as efficiently.

Frequently, the performance tradeoff is quite complex. Consider again the careful file transfer on an unreliable network. The usual technique for increasing packet reliability is some sort of per-packet error check with a retry protocol. This mechanism can be implemented either in the communication subsystem or in the careful file transfer application. For example, the receiver in the careful file transfer can periodically compute the checksum of the portion of the file thus far received and transmit this back to the sender. The sender can then restart by retransmitting any portion that arrived in error.

The end-to-end argument does not tell us where to put the early checks, since either layer can do this performance-enhancement job. Placing the early retry protocol in the file transfer application simplifies the communication system, but may increase overall cost, since the communication system is shared by other applications and each application must now provide its own reliability enhancement. Placing the early retry protocol in the communication system may be more efficient, since it may be performed inside the network on a hop-by-hop basis, reducing the delay involved in correcting a failure. At the same time, there may be some application that finds the cost of the enhancement is not worth the result but it now has no choice in the matter* . A great deal of information about system implementation is needed to make this choice intelligently.

Other examples of the end-to-end argument

Delivery guarantees

The basic argument that a lower-level subsystem that supports a distributed application may be wasting its effort providing a function that must by nature be implemented at the application level anyway can be applied to a variety of functions in addition to reliable data transmission. Perhaps the oldest and most widely known form of the argument concerns acknowledgement of delivery. A data communication network can easily return an acknowledgement to the sender for every message delivered to a recipient. The ARPANET, for example, returns a packet known as "Request For Next Message" (RFNM)[1] whenever it delivers a message. Although this acknowledgement may be useful within the network as a form of congestion control (originally the ARPANET refused to accept another message to the same target until the previous RFNM had returned) it was never found to be very helpful to applications using the ARPANET. The reason is that knowing for sure that the message was delivered to the target host is not very important. What the application wants to know is whether or not the target host acted on the message; all manner of disaster might have struck after message delivery but before completion of the action requested by the message. The acknowledgement that is really desired is an end-to-end one, which can be originated only by the target application – "I did it", or "I didn't."

Another strategy for obtaining immediate acknowledgements is to make the target host sophisticated enough that when it accepts delivery of a message it also accepts responsibility for guaranteeing that the message is acted upon by the target application. This approach can eliminate the need for an end-to-end acknowledgement in some, but not all applications. An end-to-end acknowledgement is still required for applications in which the action requested of the target host should be done only if similar actions requested of other hosts are successful. This kind of application requires a two-phase commit protocol[5,10,15], which is a sophisticated end-to-end acknowledgement. Also, if the target application may either fail or refuse to do the requested action, and thus a negative acknowledgement is a possible outcome, an end-to-end acknowledgement may still be a requirement.

Secure transmission of data

Another area in which an end-to-end argument can be applied is that of data encryption. The argument here is threefold. First, if the data transmission system performs encryption and decryption, it must be trusted to manage securely the required encryption keys. Second, the data will be in the clear and thus vulnerable as it passes into the target node and is fanned out to the target application. Third, the *authenticity* of the message must still be checked by the application. If the application performs end-to-end encryption, it obtains its required authentication check, it

---

* For example, real time transmission of speech has tighter constraints on message delay than on bit-error rate. Most retry schemes significantly increase the variability of delay.

can handle key management to its satisfaction, and the data is never exposed outside the application.

Thus, to satisfy the requirements of the application, there is no need for the communication subsystem to provide for automatic encryption of all traffic. Automatic encryption of all traffic by the communication subsystem may be called for, however, to ensure something else – that a misbehaving user or application program does not deliberately transmit information that should not be exposed. The automatic encryption of all data as it is put into the network is one more firewall the system designer can use to ensure that information does not escape outside the system. Note however, that this is a different requirement from authenticating access rights of a system user to specific parts of the data. This network-level encryption can be quite unsophisticated – the same key can be used by all hosts, with frequent changes of the key. No per-user keys complicate the key management problem. The use of encryption for application-level authentication and protection is complementary. Neither mechanism can satisfy both requirements completely.

Duplicate message suppression

A more sophisticated argument can be applied to duplicate message suppression. A property of some communication network designs is that a message or a part of a message may be delivered twice, typically as a result of time-out-triggered failure detection and retry mechanisms operating within the network. The network can provide the function of watching for and suppressing any such duplicate messages, or it can simply deliver them. One might expect that an application would find it very troublesome to cope with a network that may deliver the same message twice; indeed it is troublesome. Unfortunately, even if the network suppresses duplicates, the application itself may accidentally originate duplicate requests, in its own failure/retry procedures. These application level duplications look like different messages to the communication system, so it cannot suppress them; suppression must be accomplished by the application itself with knowledge of how to detect its own duplicates.

A common example of duplicate suppression that must be handled at a high level is when a remote system user, puzzled by lack of response, initiates a new login to a time-sharing system. For another example, most communication applications involve a provision for coping with a system crash at one end of a multi-site transaction: reestablish the transaction when the crashed system comes up again. Unfortunately, reliable detection of a system crash is problematical: the problem may just be a lost or long-delayed acknowledgement. If so, the retried request is now a duplicate, which only the application can discover. Thus the end-to-end argument again: if the application level has to have a duplicate-suppressing mechanism anyway, that mechanism can also suppress any duplicates generated inside the communication network, so the function can be omitted from that lower level. The same basic reasoning applies to completely omitted messages as well as to duplicated ones.

Guaranteeing FIFO message delivery

Ensuring that messages arrive at the receiver in the same order they are sent is another function usually assigned to the communication subsystem. The mechanism usually used to achieve such first-in, first-out (FIFO) behavior guarantees FIFO ordering among messages sent on the same virtual circuit. Messages sent along independent virtual circuits, or through intermediate processes outside the communication subsystem may arrive in an order different from the order sent. A distributed application in which one node can originate requests that initiate actions at several sites cannot take advantage of the FIFO ordering property to guarantee that the actions requested occur in the correct order. Instead, an independent mechanism at a higher level than the communication subsystem must control the ordering of actions.

Transaction management

We have now applied the end-to-end argument in the construction of the SWALLOW distributed data storage system[15], where it leads to significant reduction in overhead. SWALLOW provides data storage servers called repositories that can be used remotely to store and retrieve data. Accessing data at a repository is done by sending it a message specifying the object to be accessed, the version, and type of access (read/write), plus a value to be written if the access is a write. The underlying message communication system does not suppress duplicate messages, since a) the object identifier plus the version information suffices to detect duplicate writes, and b) the effect of a duplicate read request message is only to generate a duplicate response, which is easily discarded by the originator. Consequently, the low-level message communication protocol is significantly simplified.

The underlying message communication system does not provide delivery acknowledgement either. The acknowledgement that the originator of a write request needs is that the data was stored safely. This acknowledgement can be provided only by high levels of the SWALLOW system. For read requests, a delivery acknowledgement is redundant, since the response containing the value read is sufficient acknowledgement. By eliminating delivery acknowledgements, the number of messages transmitted is halved. This message reduction can have a significant effect on both host load and network load, improving performance. This same line of reasoning has also been used in development of an experimental protocol for remote access to disk records[6]. The resulting reduction in path length in lower-level protocols was important in maintaining good performance on remote disk access.

Identifying the ends

Using the end-to-end argument sometimes requires subtlety of analyis of application requirements. For example, consider a computer communication network that carries some packet voice connections, conversations between digital telephone instruments. For those connections that carry voice packets, an unusually strong version of the end-to-end argument applies: if low levels of the communication system try to accomplish bit-perfect communication, they will probably introduce uncontrolled delays in packet delivery, for example, by requesting retransmission of damaged packets and holding up delivery of later packets until earlier ones have been correctly retransmitted. Such delays are disruptive to the voice application, which needs to feed data at a constant rate to the listener. It is better to accept slightly damaged packets as they are, or even to replace them with silence, a duplicate of the previous packet, or a noise burst. The natural redundancy of voice, together with the high-level error correction procedure in which one participant says "excuse me, someone dropped a glass. Would you please say that again?" will handle such dropouts, if they are relatively infrequent.

However, this strong version of the end-to-end argument is a property of the specific application – two people in real-time conversation – rather than a property, say, of speech in general. If one considers instead a speech message system, in which the voice packets are stored in a file for later listening by the recipient, the arguments suddenly change their nature. Short delays in delivery of packets to the storage medium are not particularly disruptive so there is no longer any objection to low-level reliability measures that might introduce delay in order to achieve reliability. More important, it is actually helpful to this application to get as much accuracy as possible in the recorded message, since the recipient, at the time of listening to the recording, is not going to be able to ask the sender to repeat a sentence. On the other hand, with a storage system acting as the receiving end of the voice communication, an end-to-end argument does apply to packet ordering and duplicate suppression. Thus the end-to-end argument is not an absolute rule, but rather a guideline that helps in application and protocol design analysis; one must use some care to identify the end points to which the argument should be applied.

History, and application to other system areas

The individual examples of end-to-end arguments cited in this paper are not original; they have accumulated over the years. The first example of questionable intermediate delivery acknowledgements noticed by the authors was the "wait" message of the M.I.T. Compatible Time-Sharing System, which the system printed on the user's terminal whenever the user entered a command[3]. (The message had some value in the early days of the system, when crashes and communication failures were so frequent that intermediate acknowledgements provided some needed reassurance that all was well.)

The end-to-end argument relating to encryption was first publicly discussed by Branstad in a 1973 paper[2]; presumably the military security community held classified discussions before that time. Diffie and Hellman[4] and Kent[8] develop the arguments in more depth, and Needham and Schroeder[11] devised improved protocols for the purpose.

The two-phase-commit data update protocols of Gray[5], Lampson and Sturgis[10] and Reed[13] all use a form of end-to-end argument to justify their existence; they are end-to-end protocols that do not depend for correctness on reliability, FIFO sequencing, or duplicate suppression within the communication system, since all of these problems may also be introduced by other system component failures as well. Reed makes this argument explicitly in the second chapter of his Ph.D. thesis on decentralized atomic actions[14].

End-to-end arguments are often applied to error control and correctness in application systems. For example, a banking system usually provides high-level auditing procedures as a matter of policy and legal requirement. Those high-level auditing procedures will uncover not only high-level mistakes such as performing a withdrawal against the wrong account, it will also detect low-level mistakes such as coordination errors in the underlying data management system. Therefore a costly algorithm that absolutely eliminates such coordination errors may be arguably less appropriate than a less costly algorithm that just makes such errors very rare. In airline reservation systems, an agent can be relied upon to keep trying, through system crashes and delays, until a reservation is either confirmed or refused. Lower level recovery procedures to guarantee that an unconfirmed request for a reservation will survive a system crash are thus not vital. In telephone exchanges, a failure that could cause a single call to be lost is considered not worth providing explicit recovery for, since the caller will probably replace the call if it matters[7]: All of these design approaches are examples of the end-to-end argument being applied to automatic recovery.

Much of the debate in the network protocol community over datagrams, virtual circuits, and connectionless protocols is a debate about end-to-end arguments. A modularity argument prizes a reliable, FIFO sequenced, duplicate-suppressed stream of data as a system component that is easy to build on, and that argument favors virtual circuits. The end-to-end argument claims that centrally-provided versions of each of those functions will be incomplete for some applications, and those applications will find it easier to build their own version of the functions starting with datagrams.

A version of the end-to-end argument in a non-communication application was developed in the 1950's by system analysts whose responsibility included reading and writing files on large numbers of magnetic tape reels. Repeated attempts to define and implement a "reliable tape subsystem" repeatedly foundered, as flaky tape drives, undependable system operators, and system crashes conspired against all narrowly focused reliability measures. Eventually, it became standard practice for every application to provide its own application-dependent checks and recovery strategy; and to assume that lower-level error detection mechanisms at best reduced the frequency with which the higher-level checks failed. As an example, the Multics file backup system[17], even though it is built on a foundation of a magnetic tape subsystem format that

provides very powerful error detection and correction features, provides its own error control in the form of record labels and multiple copies of every file.

The arguments that are used in support of reduced instruction set computer (RISC) architecture are similar to end-to-end arguments. The RISC argument is that the client of the architecture will get better performance by implementing exactly the instructions needed from primitive tools; any attempt by the computer designer to anticipate the client's requirements for an esoteric feature will probably miss the target slightly and the client will end up reimplementing that feature anyway. (We are indebted to M. Satyanarayanan for pointing out this example.)

Lampson, in his arguments supporting the "open operating system,"[9] uses an argument similar to the end-to-end argument as a justification. Lampson argues against making any function a permanent fixture of lower-level modules; the function may be provided by a lower-level module but it should always be replaceable by an application's special version of the function. The reasoning is that for any function you can think of, at least some applications will find that by necessity they must implement the function themselves in order to meet correctly their own requirements. This line of reasoning leads Lampson to propose an "open" system in which the entire operating system consists of replaceable routines from a library. Such an approach has only recently become feasible in the context of computers dedicated to a single application. It may be the case that the large quantity of fixed supervisor function typical of large-scale operating systems is only an artifact of economic pressures that demanded multiplexing of expensive hardware and therefore a protected supervisor. Most recent system "kernelization" projects, in fact, have focused at least in part on getting function out of low system levels[16,12]. Though this function movement is inspired by a different kind of correctness argument, it has the side effect of producing an operating system that is more flexible for applications, which is exactly the main thrust of the end-to-end argument.

Conclusions

End-to-end arguments are a kind of "Occam's razor" when it comes to choosing the functions to be provided in a communication subsystem. Because the communication subsystem is frequently specified before applications that use the subsystem are known, the designer may be tempted to "help" the users by taking on more function than necessary. Awareness of end-to-end arguments can help to reduce such temptations.

It is fashionable these days to talk about "layered" communication protocols, but without clearly defined criteria for assigning functions to layers. Such layerings are desirable to enhance modularity. End-to-end arguments may be viewed as part of a set of rational principles for organizing such layered systems. We hope that our discussion will help to add substance to arguments about the "proper" layering.

Acknowledgements

Many people have read and commented on an earlier draft of this paper, including David Cheriton, F.B. Schneider, and Liba Svobodova. The subject was also discussed at the ACM Workshop in Fundamentals of Distributed Computing, in Fallbrook, California during December 1980. Those comments and discussions were quite helpful in clarifying the arguments.

References

1. Bolt Beranek and Newman Inc. Specifications for the interconnection of a host and an IMP. Technical Report No. 1822, Cambridge, Mass., December, 1981.
2. Branstad, D.K. Security aspects of computer networks. AIAA Paper No. 73-427, AIAA Computer Network Systems Conference, Huntsville, Alabama, April, 1973.
3. Corbato, F.J., et al. *The Compatible Time-Sharing System, A Programmer's Guide*. M.I.T. Press, Cambridge, Massachusetts, 1963, p.10.
4. Diffie, W., and Hellman, M.E. New directions in cryptography. *IEEE Trans. on Info. Theory*, IT-22, 6, (November, 1976), pp.644-654.
5. Gray, J.N. Notes on database operating systems. In *Operating System: An Advanced Course.* Volume 60 of *Lecture Notes in Computer Science*, Springer-Verlag, 1978, pp.393-481.
6. Greenwald, M. Remote virtual disk protocol specifications. M.I.T. Laboratory for Computer Science Technical Memorandum, in preparation. Expected publication, 1984.
7. Keister, W., Ketchledge, R.W., and Vaughan, H.E.: No. 1 ESS: System organization and objectives. *Bell System Technical Journal 53*, 5 (part 1), (September, 1964) p. 1841.
8. Kent, S.T.: Encryption-based protection protocols for interactive user-computer communication.: S.M. thesis, Massachusetts Institute of Technology, Department of Electrical Engineering and Computer Science, May, 1976. Also available as M.I.T. Laboratory for Computer Science Technical Report, TR-162, May, 1976.
9. Lampson, B.W., and Sproull, R.F. An open operating system for a single-user machine. *Proc. Seventh Symposium on Operating Systems Principles, Operating Systems Review 13*, Special issue (December, 1979), pp.98-105.
10. Lampson, B., and Sturgis, H: Crash recovery in a distributed data storage system. Working paper, Xerox PARC, November, 1976 and April, 1979. Submitted to *CACM.*
11. Needham, R.M., and Schroeder, M.D.: Using encryption for authentication in large networks of computers. *CACM 21*, 12, (December, 1978), pp.993-999.
12. Popek, G.J., et al.: UCLA data secure unix. *Proc. 1979 NCC*, AFIPS Press, pp.355-364.
13. Reed, D.P.: Implementing atomic actions on decentralized data. *ACM Transactions on Computer Systems 1*, 1 (February, 1983), pp.3-23.
14. Reed, D.P.: Naming and synchronization in a decentralized computer system. Ph.D. thesis, Massachusetts Institute of Technology, Department of Electrical Engineering and Computer Science, September 1978. Also available as M.I.T. Laboratory for Computer Science Technical Report, TR-205, September, 1978.
15. Reed, D.P., and Svobodova, L.: SWALLOW: A distributed data storage system for a local network. In West, A., and Janson, P., ed. *Local Networks for Computer Communications, Proc. IFIP Working Group 6.4 International Workshop on Local Networks*. North-Holland, Amsterdam, 1981, pp.355-373.
16. Schroeder, M.D., Clark, D.D., and Saltzer, J.H.: The Multics kernel design project. *Proc. Sixth Symposium on Operating Systems Principles, Operating Systems Review 11*, 5 (November, 1977,) pp.43-56.
17. Stern, J.A.: Backup and recovery of on-line information in a computer utility. S.M. thesis, M.I.T. Department of Electrical Engineering and Computer Science, August 1973. Available as M.I.T. Project MAC Technical Report TR-116, January, 1974.

Prepared Statement of
Vinton G. Cerf
Vice President and Chief Internet Evangelist
Google Inc.

U.S. Senate Committee on Commerce, Science, and Transportation
Hearing on
"Network Neutrality"

February 7, 2006

Good morning Chairman Stevens, Senator Inouye, and members of the Committee. My name is Vint Cerf, and I am currently Vice President and Chief Internet Evangelist with Google. You may be more familiar with me for my work over the last few decades as one of the network engineers involved in devising the software protocols that underpin the Internet. Thank you for inviting me here today to discuss the important concept of network neutrality. As this Committee considers the future of U.S. communications law, it faces choices linked inexorably to important American values: consumer choice, economic opportunity, and technological innovation. In turn the way we approach those policy choices will have a tremendous impact on our ability as a nation to compete effectively on a global stage. In short, I appreciate the opportunity to share some of my thoughts about issues affecting nothing less than the future of the Internet.

I. Introduction and overview

The Internet's open, neutral architecture has proven to be an enormous engine for market innovation, economic growth, social discourse, and the free flow of ideas. The remarkable success of the Internet can be traced to a few simple network principles – end-to-end design, layered architecture, and open standards -- which together give consumers choice and control over their online activities. This "neutral" network has supported an explosion of innovation at the edges of the network, and the growth of companies like Google, Yahoo, eBay, Amazon, and many others. Because the network is neutral, the creators of new Internet content and services need not seek permission from carriers or pay special fees to be seen online. As a result, we have seen an array of unpredictable new offerings – from Voice-over-IP to wireless home networks to blogging – that might never have evolved had central control of the network been required by design.

Allowing broadband carriers to control what people see and do online would fundamentally undermine the principles that have made the Internet such a success. For the foreseeable future most Americans will face little choice among broadband carriers. Enshrining a rule that permits carriers to discriminate in favor of certain kinds or sources of services would place those carriers in control of online activity. Allowing broadband carriers to reserve huge amounts of bandwidth for their own services will not give consumers the broadband Internet our country and economy need. Promoting an open and accessible Internet is critical for consumers. It is also critical to our nation's competitiveness – in places like Japan, Korea, Singapore, and the United Kingdom, higher-bandwidth and *neutral* broadband platforms are unleashing waves of innovation that threaten to leave the U.S. further and further behind.

My testimony will explain briefly why network neutrality has been so important to the Internet's success and should be preserved. Among its key points:

- The Internet was designed to maximize user choice and innovation, which has led directly to an explosion in consumer benefits. The use of layered architecture, end-to-end design, and the ubiquitous Internet Protocol standard, together allow for the decentralized and open Internet that we have come to expect. This created an environment that did not require Tim Berners-Lee to seek permission from the network owners before unveiling a piece of software enabling the World Wide Web.

- Most American consumers today have few choices for broadband service. Phone and cable operators together control 98 percent of the broadband market, and only about half of consumers actually have a choice between even two providers. Unfortunately, there appears to be little near-term prospect for meaningful competition from alternative platforms. As a result, the incumbent broadband carriers are in position to dictate how consumers and producers can use the on-ramps to the Internet.

- A number of justifications have been created to support carrier control over consumer choices online; none stand up to scrutiny. Open-ended carrier discrimination is not needed to protect users from viruses, stop spam, preserve network integrity, make VOIP or video service work properly – or even insure that carriers are compensated for their broadband investments. In particular, we firmly believe that carriers will be able to set market prices for Internet access and be well-paid for their investments – as broadband carriers in other countries have successfully done.

- Even as we welcome the deregulation of our telecommunications system, we must preserve some limited elements of openness and non-discrimination that have long been part of our telecommunications law. In this regard, Google supports tailored, minimally-intrusive safeguards to promote net neutrality. Legislative approaches in both chambers have helpfully acknowledged the need for some form of net neutrality. We look forward to helping strengthen those provisions to provide the safeguards needed.

Google believes that consumer should be able to use the Internet connections that they pay for the way that they want. This principle – that users pick winners and losers in the Internet marketplace, not carriers – is an architectural and policy choice critical to innovation online. Google itself is a product of the Internet. We care passionately about the future of the Net, not just for ourselves, but because of all the other potential Googles out there. Indeed, we are not alone: Our concerns are shared by Internet companies, small businesses, end users, and consumer groups across the country. The vibrant ecosystem of innovation that lies at the heart of the Internet creates wealth and opportunity for millions of Americans. That ecosystem – based upon a neutral open network -- should be nourished and promoted.

Mr. Chairman, Google commends you and the members of this Committee for your thoughtful leadership and attention in this area, and we look forward to working closely with you in the weeks and months ahead.

II. The lasting lessons of the Internet

Some believe that the Internet was born and flourished out of a fortuitous accident, a random interaction of market forces and technology. But that simply is not the case.

The advent of the Internet took tremendous vision and initiative, by numerous network engineers, and software developers, and hardware vendors, and entrepreneurs. That advent also included visionary U.S. policymakers who recognized that the government largely needed to get out of the way, and allow the free market to work its genius in this new interactive, online environment. At the same time, as I will explain below, that policy judgment rested on an existing regulatory framework that allowed open and nondiscriminatory access to the Internet.

I was fortunate to be involved in the earliest days of the "network of networks." From that experience, I can attest to how the actual design of the Internet – the way its digital hardware and software protocols, including the TCP/IP suite, were put together -- led to its remarkable economic and social success.

First, the layered nature of the Internet describes the "what," or its overall structural architecture. The use of layering means that functional tasks are divided up and assigned to different software-based protocol layers. For example, the "physical" layers of the network govern how electrical signals are carried over a physical medium, such as copper wire or radio waves. The "transport" layers help route the user's data packets to their correct destinations, while the application layers control how those packets are used by a consumer's email program, web browser, or other computer application. This simple and flexible system creates a network of modular "building blocks," where applications or protocols at higher layers can be developed or modified with no impact on lower layers, while lower layers can adopt new transmission and switching technologies without requiring changes to upper layers. Reliance on a layered system greatly facilitates the unimpeded delivery of packets from one point to another.

Second, the end-to-end design principle describes the "where," or the place for network functions to reside in the layered protocol stack. With the Internet, decisions were made to allow the control and intelligence functions to reside largely with users at the "edges" of the network, rather than in the core of the network itself. For example, it is the user's choice what security to use for his or her communications, what VOIP system to use in assembling digital bits into voice communications, or what web browser to adopt. This is precisely the opposite of the traditional telephony and cable networks, where control over permitted applications is handled in the core (in headends and central offices), away from the users at the edge. As a result, the power and functionality of the Internet is left in the hands of the end users.

Third, the design of the Internet Protocol, or the "how," allows for the separation of the networks from the services that ride on top of them. IP was designed to be an open standard, so that anyone could use it to create new applications and new networks (by nature, IP is completely indifferent to both the underlying physical networks, and to the countless applications and devices using those networks). As it turns out, IP quickly became the ubiquitous bearer protocol at the center of the Internet. Thus, using IP, individuals are free to create new and innovative applications that they know will work on the network in predictable ways.

Finally, from these different yet related design components, one can see the overarching rationale -- the "why" -- that no central gatekeeper should exert control over the Internet. This governing principle allows for vibrant user activity and creativity to occur at the network edges. In such an environment, entrepreneurs need not worry about getting permission for their inventions will reach

the end users. In essence, the Internet has become a platform for innovation. One could think of it like the electric grid, where the ready availability of an open, standardized, and stable source of electricity allows anyone to build and use a myriad of different electric devices. This is a direct contrast to closed networks like the cable video system, where network owners control what the consumer can see and do.

In addition to this architectural design, the Internet has thrived because of an underlying regulatory framework that supported openness. Wisely, government has largely avoided regulating the Internet directly. Google firmly supports this deregulatory approach, which is supported by the openness and consumer choices available in this new medium. At the same time, the underlying network through which consumers access the Internet has rested on a telecommunications regulations that ensured openness – including a century's-old tradition in American law that telephone companies are not allowed to tell consumers who they can call or what they can say.

In the zone of governmental noninterference surrounding the Internet, one crucial exception had been the nondiscrimination requirements for the so-called last mile. Developed by the FCC over a decade before the commercial advent of the Internet, these "Computer Inquiry" safeguards required that the underlying providers of last-mile network facilities – the incumbent local telephone companies – allow end users to choose any ISP, and utilize any device, they desired. In turn, ISPs were allowed to purchase retail telecommunications services from the local carriers on nondiscriminatory rates, terms, and conditions.

The end result was, paradoxically, a regulatory safeguard applied to last-mile facilities that allowed the Internet itself to remain open and "unregulated" as originally designed. Indeed, it is hard to imagine the innovation and creativity of the commercial Internet in the 1990s ever occurring without those minimal but necessary safeguards already in place. By removing any possibility of ILEC barriers to entry, the FCC paved the way for an explosion in what some have called "innovation without permission." A generation of innovators -- like Tim Berners-Lee with the World Wide Web, Yair Goldfinger with Instant Messaging, David Filo and Jerry Yang with Yahoo!, Jeff Bezos with Amazon, and Larry Page and Sergey Brin with Google – were able to offer new applications and services to the world, without needing permission from network operators or paying exorbitant carrier rents to ensure that their services were seen online. And we all have benefited enormously from their inventions.

III. The challenge posed by a concentrated broadband market

As we move to a broadband consumer network, the Internet's openness is being threatened. Most consumers face few choices among broadband carriers, giving carriers tremendous market power. At the same time, the FCC has shown little willingness to extend the long-standing non-discrimination rules governing our telecommunications system to the incumbent broadband providers. As a result, carriers increasingly will have an economic incentive to use their power to block competitors, seek extra payments to ensure that Internet content can be seen, and generally control consumer activity online.

Were there sufficient competition among and between various broadband networks, Google's concerns about the future of the Internet would largely be allayed. Unfortunately, the FCC's own figures demonstrate the significant degree of concentration in the broadband market. In 2004, the Commission reported that only 53 percent of Americans have a choice between cable modem service and DSL service. Of the remaining consumers, 28 percent have only one choice, and 19 percent have no choice at all. Thus, nearly half of all consumers lack meaningful choice in broadband providers.

Moreover, the alternatives to DSL and cable modem service remain a very small part of the market. As of December 2004, the FCC's figures show that incumbent cable and telephone company broadband services together constitute 98.7 percent of the total market. This leaves only 1.3 percent of the current market for alternative broadband networks such as wireless, satellite, and BPL. Shockingly, the share of alternative networks has *shrunken* steadily, from 2.9 percent in December 1999. Thus, even the FCC's own figures demonstrate that there are only two dominant and only partially-competitive modalities – cable and telco -- and a tiny and declining share of third modalities.[1]

To me, as a scientist, it comes down ultimately to questions of physics and economics. First, can such alternative networks be built, given the limitations of available network atoms and radio spectrum? Second, will such alternative networks be built, given the immense time and effort involved? Whether we are discussing BPL or WiMax or satellite, the prospect of a near-term, ubiquitous competing broadband platform does not appear promising.

In the absence of any meaningful competition in the consumer broadband market, and without the user safeguards that have governed similar last-mile competition to date, one would expect carriers to have an economic incentive – and the opportunity -- to control users' online activity. Not surprisingly, this incentive is already manifesting itself. Just last spring, the FCC found that the Madison River Telephone Company was blocking ports used by its DSL customers to access competing VoIP services.[2] Similar examples are emerging internationally as well. More revealingly, in recent months senior executives of major U.S. carriers have indicated publicly that they intend to force competing services and content providers to pay to be seen online.[3] Together, these examples show that carrier discrimination is not a hypothetical concern.

IV. Debunking the ever-changing rationale for network discrimination

Recently, various justifications have been offered to explain why carriers need to limit the ability of end users to control their own connections to the Internet. For years many broadband carriers insisted that they would never discriminate against application providers, or limit their customers' access to the Internet. More recent arguments for carrier discrimination have included the need to insert network controls to protect their customers against spam and other security threats, or to insure the quality of VoIP services. Now they argue that their IP video services will require substantial bandwidth that otherwise would be used by Internet applications. They also have decided to look to

---

[1] AT&T CEO Ed Whitacre also has acknowledged the highly concentrated nature of the consumer broadband market. In a recent interview with Business Week, he noted that in the broadband space, "it's still about scale and scope. It's about owning the assets that connect customers. The assets that probably can't be duplicated except maybe by the cable companies." Certainly the FCC's numbers bear that out.

[2] Federal Communications Commission, In the Matter of Madison River Communications, LLC and affiliated companies, Order, File No. EB-05-IH-0110, adopted March 3, 2005.

[3] Just three months ago, AT&T CEO Edward Whitacre observed that only telephone carriers and cable companies have broadband pipes to customers. He insisted that Google and other companies "use my lines for free, and that's bull." He then warned that "I ain't going to let them do that" because "there's going to have to be some mechanism for these people who use these pipes to pay for the portion they're using." *Rewired and Ready for Combat*, BUSINESS WEEK ONLINE, November 7, 2005; *Online Extra: At SBC, It's All About "Scale and Scope*, BUSINESS WEEK ONLINE, November 7, 2005. As noted below, Mr. Whitacre's economic theories leave something to be desired.

applications providers such as Google to help pay for the expense involved in providing broadband networks - and that any attempts to curtail their network control will remove their incentives to continue investing. None of these justifications stands up under close scrutiny.

- Network neutrality need not prevent anyone – carriers or applications provider – from developing software solutions to remedy end user concerns such as privacy, security, and quality of service. The issue arises where the network operator decides to place the functionality in the physical or logical layers of the network, rather than in the application layer where they belong. Such a move is contrary to many of the fundamental architectural principles of the Internet. In particular, attempting to solve applications issues at the physical layer violates the layered, modular nature of the Net. With a few very narrowly-tailored exceptions – such as defending against network-level denial of service attacks or router attacks – altering or blocking packets within the network is inconsistent with the end-to-end design principle. The end result is the insertion of a gatekeeper that – even arguably under the best of intentions – disrupts the open, decentralized platform of the Internet.

- Broadband capacity is not nearly as constrained as the network owners would have us believe. Some applications, such as voice over IP, take up very little bandwidth. Other activities, such as multi-player real-time gaming or streaming video, may require more capacity. However, such applications could be subject to additional customer charges, based on the access speeds required (as opposed to the source, destination, or content of the traffic) – but without discriminating based on who is providing the service.

- The broadband carriers already are fully compensated by their residential customers for their use of the network. These companies can charge their own customers whatever they want, in order to make back their investments. Trying to extract additional fees from Web-based companies – who are not in any way "customers" of the provider -- would constitute a form of "double recovery." Google takes no issue with the broadband carriers' ability to set prices for Internet access that compensate for the costs and risks associated with their network investments.

- Some carriers are also seeking permission to create two separate IP networks: one for the public Internet and one for a privately-managed, proprietary service. Allowing segmentation of the broadband networks into capacious "broadest-band" toll lanes for some, and narrow dirt access roads for the rest, is contrary to the design and spirit behind the Internet, as well as our national competitive interests. And by definition, favoring some disfavors others. In an environment where consumers already have little to no choice of broadband providers, the end result is a cramped version of the robust and open environment we all take for granted today. Prioritization inevitably becomes a zero-sum game.

- Many seem to forget that the rational for reduced regulation at the FCC was based in part on the promise that carriers would build robust broadband platforms to support the Internet. Turning away from those commitments would undermine the rational for deregulation. Moreover, retaining some type of user safeguard that promotes an outcome of net neutrality would seem a small burden in the context of the immense deregulation that has happened, and likely will continue to happen, at the FCC.

Finally, we would do well to take important lessons from other countries. Whatever metric one uses, the United States lags behind other developed countries in the deployment and use of high-speed connections to the Internet. Ironically, many such countries employ the same principles of network openness and nondiscrimination that helped shape our own experience of the Internet. Certainly the

incumbent providers in those countries do not appear to suffer from any lack of incentives under those principles. For example, in the United Kingdom, British Telecom has agreed to split itself into a retail arm and a wholesale business, with a fundamental policy of nondiscriminatory treatment governing the relationship between them and other providers. In a number of Asian countries, both incumbent and competitive providers operating in an unbundled environment sell huge amounts of bandwidth – 100 Megabits or more per second -- at a fraction of U.S. prices. By abandoning the principles that helped foster user choice and innovation, the United States risks falling further behind in the global economy.

V. Preserving neutrality in our telecommunications law

Even as we welcome the deregulation of our telecommunications system, we should preserve some limited elements of openness and non-discrimination that have long been part of our telecommunications law. Absent real physical layer competition, Google supports a tailored, minimally-intrusive, and enforceable network neutrality rule.

Congress now is considering possible legislation in this area. We are gratified that legislative approaches in both chambers recognize the need for some form of network neutrality safeguards to protect the interests of Internet users in a concentrated broadband market. Unfortunately they do not go far enough towards creating enforceable protections against carrier interference with consumer choices.[4] Allowing broadband carriers to discriminate in favor of certain kinds of services, and to potentially interfere with others, would take control away from the end users of the Internet, and place it in the hands of those who own the network. The current draft bills take a step in the right direction, but ultimately do not go far enough to preserve the vibrant innovation at the edge of the Internet. Our concerns are shared by Internet companies, small businesses, Internet end users, and consumer groups across the country.

As Congress and the FCC consider these issues, we should establish our end goal with as much clarity as possible, and then work back from there to develop an optimal mechanism for achieving that goal. In this context, we favor an environment much like the one that gave birth to the Internet: where end users can engage in activities such as running applications, employing devices, and accessing content, unfettered by the provider of the underlying network connection. Such an environment is best engendered by retaining a public policy framework that reflects the modular, end-to-end, and open nature of the Internet.

The best long-term answer to this problem is significantly more broadband competition. Ideally, physical layer problems merit physical layer solutions. While the prospects for such "intermodal" competition remain dim for the foreseeable future, Congress should ensure that the FCC has all the tools it needs to maximize the chances for long-term success in this area.

---

[4] Last July, Senator Ensign introduced S.1504, the "Broadband Investment and Consumer Choice Act of 2005." While the focus is on establishing streamlined nationwide video franchises, the bill also contains language concerning consumer access to the Internet. In September 2005, House Commerce Committee Chairman Barton issued a draft bill, widely known as "BITS I." A revised version, "BITS II," was released in November. Both drafts include provisions requiring broadband providers to allow consumers to access content, applications, and services, and to connect devices. Both versions also contain a number of important exceptions to those duties, related to elements like value-added services and enhanced quality of service. Unfortunately, as written the exceptions in each of these bills are so broad that they undermine the underlying neutrality requirement.

We must stress here that finding a straightforward, minimally-intrusive safeguard need not deny the network operators the ability to recover their investments, and the proper incentives to further deploy their networks. In a very real way, content and application companies like Google need the high-speed access provided by broadband carriers, just as they need the attractive new Internet offerings to drive demand for that access. It is in our collective best interest for the United States to have the best broadband capabilities in the world, bar none. The prospects for continued American ingenuity and entrepreneurship deserve nothing less.

VI. Conclusion

The Internet has become an immense catalyst for economic growth and prosperity, in this country and around the world. However, our nation is risking the loss of that catalyst, just when the broadband era should be creating the most benefits for the most people. Allowing the interests of network owners to shackle the Internet could severely undercut our nation's ability to compete effectively in the global market. We must do all we can to preserve the fundamental enabling principles of the Internet: user choice, innovation, and global competitiveness.

Google looks forward to working with this Committee to fashion carefully-tailored legislative language that protects the legitimate interests of America's Internet users. And that includes the future interests of the next Google, just waiting to be born in someone's dorm room or garage.

Thank you.

Tim Wu

Network Neutrality, Broadband Discrimination
Journal of Telecommunications and High Technology Law, Vol. 2, p. 141, 2003

Network Neutrality: Competition, Innovation, and Nondiscriminatory Access
Testimony before the House Judiciary Committee

Why have a Telecommunications Law?: Anti-Discrimination Norms in Communications
Columbia Public Law Research Paper No. 06-115

The Broadband Debate: A User's Guide
Journal of Telecommunications and High Technology Law, Vol. 3, No. 69, 2004

Letter to the FCC
Ex parte letter, with Lawrence Lessig, Summer 2003

Why you should care about network neutrality
Article in Slate magazine, May 1, 2006

Keeping the Internet Neutral? Christopher S. Yoo and Timothy Wu debate
Legal Affairs, May 1, 2006

Chris Yoo

Would Mandating Broadband Network Neutrality Help or Hurt Competition? A Comment on the End-to-End Debate

Network Neutrality FAQ

Trying to figure out the network neutrality debate via the web is kind of hard. The wikipedia entry is too prone to fights and some of the other web sites are deliberately misleading. This web site is offered in the hope that it might help introduce matters and points of controversy in network neutrality. More details are found in the papers on the left.

Definition

Network neutrality is best defined as a network design principle. The idea is that a maximally useful public information network aspires to treat all content, sites, and platforms equally. This allows the network to carry every form of information and support every kind of application. The principle suggests that information networks are often more valuable when they are *less* specialized – when they are a platform for multiple uses, present and future. (For people who know more about network design, what is just described is similar to the "end-to-end" design principle).

(Note that this doesn't suggest *every* network has to be neutral to be useful. Discriminatory, private networks can be extremely useful for other purposes. What the principle suggests that there is such a thing as a neutral public network, which has a particular value that depends on its neutral nature).

A useful way to understand this principle is to look at other networks, like the electric grid, which are implicitly built on a neutrality theory. The general purpose and neutral nature of the electric grid is one of the things that make it extremely useful. The electric grid does not care if you plug in a toaster, an iron, or a computer. Consequently it has survived and supported giant waves of innovation in the appliance market. The electric grid worked for the radios of the 1930s works for the flat screen TVs of the 2000s. For that reason the electric grid is a model of a neutral, innovation-driving network.

The theory behind the network neutrality principle, which the internet sometimes gets close to, is that a neutral network should be expected to deliver the most to a nation and the world economically, by serving as an innovation platform, and socially, by facilitating the widest variety of interactions between people. The internet isn't perfect but it aspires for neutrality in its original design. Its decentralized and mostly neutral nature may account for its success as an economic engine and a source of folk culture.

Elaborating on this point – what the economic and social benefits of neutral information networks are -- has been one of the aims parts of my scholarship. In addition, other scholars such as Lawrence Lessig, Mark Lemley, Brett Frischman and Barbara van Schewick, have done much to develop these arguments.

The hard question, of course, is what exactly is "neutral?" But more on that further down.

Origins of the Debate

The Net Neutrality debate grew out of the concerns in the late 1990s about possible threats to the end-to-end nature of the internet. As documented by Mark Lemley and Lawrence Lessig in particular, the concern was that the vertical integration of cable firms with ISPs would prove a threat to the e2e design of the internet.

Journal of Telecommunications and High Technology Law, Vol. 3, 2004

Network Neutrality and the Economics of Congestion
Georgetown Law Journal, Vol. 94, June 2006, Vanderbilt Law and Economics Research Paper No. 05-28, Vanderbilt Public Law Research Paper No. 05-33

Beyond Network Neutrality
Harvard Journal of Law and Technology, Vol. 19, Fall 2005

Barbara van Schewick

Toward an Economic Framework for Network Neutrality,
Journal on Telecommunications and High Technology Law, Vol. 5, 2007

Phil Weiser

Modularity, Vertical Integration, and Open Access Policies: Towards a Convergence of Antitrust and Regulation in the Internet Age
Harvard Journal of Law and Technology, Vol. 17, No. 1, Fall 2003

A "Third Way" on Network Neutrality
The Information Technology and Innovation Foundation, May 30, 2006

Brett Frischman

An Economic Theory of Commons and Infrastructure Management
Minnesota Law Review, Vol. 89, pp. 917-1030, 2005

Jonathan Zittrain

The Generative Internet
Harv. L. Rev. (2007)

Mark Lemley & Lawrence Lessig

The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era

The Disclosure Project

http://www.dpsproject.com/

One suggested remedy was allowing consumers their choice of ISPs, usually called an "open access remedy."

Another idea was an anti-discrimination rule. This paper, Network Neutrality, Broadband Discrimination, written in 2002, argued that a discrimination rule was the best way, and in fact better than open access remedies, as a means to protect a neutral network. At some point thereafter the term network neutrality came into common usage.

The actual term "network neutrality," new or not, has a lot in common with alot of old ideas. The concept of a "common carrier," dating from 16th century English common law, captures many similar concepts. A common carrier, in its original meaning, is a private entity that performs a public function (the law was first developed around port authorities). Furthermore, in networking, the "end-to-end" principle of network design is also a close cousin, if not the direct ancestor of network neutrality. David Isenberg's lucid and well known "dumb pipe paper" is more or less the same idea.

Moreover, the basic economic problem found in the network neutrality debate (a form of "platform exclusion" or "vertical foreclosure") can be found in many other markets. In radio, for example, you have the problem of "payola" -- payments from the recording industries to radio stations, in exchange for playing their songs. Payola isn't great for music in the United States -- it is one of the reasons radio stations all sound the same.

However, I should point out that not all economists think that things like payola are actually a problem. They argue that if payola is inefficient then radio stations that don't accept payments will have an advantage, and would therefore stop, ergo, payola must be welfare maximizing.

Law

I think it's important to differentiate sharply between the *principle* of network neutrality and a network neutrality *law*. It's a mistake to equivocate the design principle with proposed legislation of various forms. A neutral network might be designed without legal prodding -- as in the original internet. In an ideal world, either competition or enlightened self-interest might drive carriers to design neutral networks.

However, when that isn't the case—when carriers are interested in discriminating for one of various reasons -- matters get more difficult, and a law may be necessary.

To my mind, laws are most successful when they combat harmful behavior. To my mind, the basic justification for any law on network neutrality is an economic justification -- preventing behavior that may be narrowly beneficial for the carrier but that has negative spillovers for the economy and the nation.

The proposals I have supported focus on the following potential problems:

1. **Blocking**

Blocking is the worst deviation from neutrality. Some economists might think it justified, but the basic problem is a distortion of competition between the blocked and unblocked companies.

2. **Termination Monopoly Pricing**

Since broadband service providers have a "termination" monopoly over the end user, they can use that to charge termination fees to those who wish to get access to the user.

3. **"Playing Favorites" or MFN (Most Favored Network?) violations**

Where carriers offer exclusive, preferential treatment to one application provider over others. Also distorting, though obviously less than blocking.

4. **Transparency Failures**

Where carriers fail to tell customers and application developers what, as far as they know, service they offer – i.e., estimated bandwidth, latency, etc.

In addition, a group have proposed rules on what can be called "Internet" service. Those might be considered a form of transparency regulation.

What's Neutral?

This is the hardest question for any advocate of network neutrality. I've always felt that carriers should be allowed to offer special services on purely private networks. That's basically, for example, what the cable TV networks do.

The question then is whether it's more neutral if carriers build networks with priority for certain content, or whether it's more neutral to treat a bit as a bit.

I think the best, although still not ideal way to think about this problem is with the help of a private/public distinction. Private networks in this sense of the word are networks that aren't interconnected with others. The cable TV network, described above, is a good example. On a private network, discrimination part of what gives the network its utility. By definition it is closed to outsiders, and that's what makes it useful. The main point is that discrimination on a private network does have effects on the broader network – it doesn't spill over.

Matters are different on a public network, or what is sometimes called an inter-network, or internet. On the internet, discrimination at one point can affect activities on other parts of the network. Hence

The best design principles leave carriers with a choice: build private networks that are discriminatory by nature (like cable, some versions of IPTV), or join the open network and play by the norms of neutrality. This is basically the status quo today.

What about the argument that the internet might profitably be improved – that the principles of network neutrality are leaving us with the network of the 1980s? Shouldn't people in this field accept that deviations from neutrality might improve the public network, and not just private networks?

This point raises a technical question: for it depends on whether you think Quality of Service guarantees are possible across a large public networks. Most agree that they work on smaller networks, but how about the entire internet? Among others, the Internet2 research group has argued that QoS systems don't work well on public networks

-- Andy Oram has a great piece explaining the development in their thinking.

If we assume that QoS generally doesn't work on public networks but does work well on private networks then we reach a common conclusion: the neutrality principle's main exception needs to be for private networks. It may be better for the entire network's design to distinguish between what's generally public, and what's private, and treat each network differently.

Relationship to Market Power

Another hard policy question is whether network neutrality rules (or laws) are called for in the absence of market power and concentration. As discussed above, network neutrality is first and foremost a principle. Therefore, in a market where vigorous competition exists, will the market itself solve any problems of discrimination?

I don't want to try and answer the question on this web page – I address it more fully in my writings at left. But suffice to say, whether neutrality rules might still be useful given vigorous competition is an open question.

Conclusion

This short page can only introduce the concept of network neutrality and flesh out a few ideas. For more in depth work, read the works referenced in the margin.

<new page r/v>
<set drop folio>

Susan Crawford

Excerpt from *Captive Audience* (forthcoming 2013)

Chapter 2
Regulatory Pendulum
The Long Twilight Struggle

[Beginning sections of this chapter removed]

The 1996 Telecommunications Act

Here are the conditions that shaped the 1996 act: the Baby Bells were demanding permission to compete with the cable companies and to offer long-distance services. The cable companies were finding ways to continue to overcharge consumers. Consumers wanted competition for local phone service. And congressional power now belonged to the Republicans.

The 1996 act set up a grand bargain: it tried to force competition into all telecommunications markets while also deregulating them. The Bells had to give smaller companies access to their circuits, and the cable companies had to allow the Bells to compete with them for cable service. Local telephone companies could now offer long-distance service outside their own service areas, but in order to offer long distance inside their service areas, they had to prove that they had opened their local phone markets to competition. Rate regulation for cable systems was ended other than for the "basic tier" of programs; the theory was that stiffer competition from telephone companies (now in the video business) would constrain rates.[46]

Congress did leave in place an FCC requirement that limited the percentage of the market that one cable provider could control to 30 percent of all pay-TV subscribers. The FCC argued that the 30-percent-ownership limit was "generally appropriate to prevent the nation's largest MSOs [multiple systems operators--that is, the cable companies] from gaining enhanced leverage from increased horizontal concentration," while ensuring that "the majority of MSOs continue[d] to expand and benefit from the economies of scale necessary to encourage investment in new video programming services and the deployment of advanced cable technologies."[47]

What the act did not do was keep the cable companies from clustering their operations ("you take Minnesota, I'll take Sacramento") or the telephone companies from consolidating. Even before it passed, two of the Baby Bells, NYNEX and Bell Atlantic, were rumored by the Wall Street Journal to be considering a merger. Within a few years, the Baby Bells were merging rapidly: SBC bought Pacific Telesis, then Bell Atlantic and NYNEX merged. There was activity in long-distance markets as well: AT&T bought Teleport, and MCI bought a metropolitan fiber network called MFS. Bell Atlantic merged with GTE and renamed itself Verizon. SBC bought Ameritech. By 2005 America was effectively left with two wired companies--Verizon and SBC.[48]

At the same time, MCI and the old AT&T (still in long distance) kept trying to enter local markets and were having a hard time. They faced a firestorm of litigation over the regulations the FCC had created to force incumbents to share their facilities with their competitors. Essentially, the Baby Bells used the courts to avoid the act's requirement that they open up their local networks to competition. The ensuing litigation went on for ten years. When it was over, the 1996 effort to open up phone lines to competition was widely considered a failure. In the end, the D.C. Circuit and the FCC so softened SBC's obligation to lease its facilities that AT&T had effectively no chance to get into local competition with the Baby Bells. The regulators had been thoroughly out-lawyered.[49]

AT&T gave up and announced in January 2005 that it would be bought by SBC--and bringing everything full circle, SBC renamed the new entity AT&T. Verizon acquired MCI at the same time. Both Verizon and SBC claimed that they could increase efficiency by combining long-distance with local phone services, but whether those cost savings would be passed along to consumers was not clear.[50] The new AT&T, as an integrated company, saw "positive indications of pricing stability" after the merger. In other words, competition would not be a problem.[51]

What had happened to the competition that the 1996 law was supposed to foster? The act's fundamental assumption, that open platforms and alternative technologies would undermine the market power of the incumbent carriers over basic communications platforms--and that behavioral regulations on these actors would make structural limitations unnecessary--has proven overly optimistic. Although the phone companies were supposed to allow competing carriers to share their facilities, and the cable companies were supposed to compete with the phone companies to provide distribution of video content, data, and phone services, the opposite happened. On the phone side, without limits on mergers, consolidation and litigation foiled the act's open-access mandates. At the same time, cross-technology competition between phone and cable turned out to be weak: when it came to wired access, the incumbent cable operators had unbeatable economic advantages over the phone companies.

Internet access, a service provided by both phone and cable companies, could have disrupted all these giant companies' efforts to block competition, if only the open-access mandates of the act had held firm. But the mergers were not what undermined the power of Internet access to eliminate the gatekeeping role that the carriers enjoyed. Given all those years of litigation over the precise meaning of this word and that in the 1996 act, it is understandable that the new FCC chair in 2001 would look for a way to cut through the knot.
<ls>

Michael Powell, chairman of the FCC from 2001 to 2005 and now the leader of the cable industry's trade association, has an easy speaking style. He is clearly aware of the overstated rhetoric that often characterizes titanic battles over telecommunications policy and is happy to follow suit in his tone and choice of words. He raises his eyebrows, makes his points lightly, speaks blazingly fast, and moves on. He often told reporters that he was enjoying being the FCC chairman, and he seemed to mean it.

Powell was born in 1963 in Birmingham, Alabama, and as the only son of General Colin Powell, he heard the call to public duty at a young age. Scholarly by temperament but convinced of the importance of the armed forces, he enlisted in the army after college and suffered a broken back when the jeep he was in crashed in a rainstorm and rolled over on him; he was flown back to Washington and spent more than a year recuperating. Law school, an appellate clerkship, private practice, and a stint as chief of staff at the Antitrust Division launched his public career. During the Clinton administration he was named an FCC commissioner, and he became chairman when his party came to power in January 2001.

Powell is a genuine student of technology who was convinced early on of the transformative power of the Internet. He downloaded Skype as soon as it was released. On his arrival at the FCC, he was shocked to find that 40 percent of the staff engineers were close to retirement. Powell brought an intellectual, inquiring joy to his role at the commission, setting up "FCC University" to ensure that all staff members understood the technologies and economic questions they were dealing with. As he explained in 2002, "I wanted the FCC University to be the very best employee development program that anyone can find in the US government."[52] Robert Pepper, who served as a policy adviser to six FCC chairmen between 1989 and 2005, said during the Powell chairmanship, "Out of the modern chairmen, Michael Powell is the most technologically sophisticated. He absolutely understands the power of technology. He invested in technology at the FCC--we hired new engineers, we revitalized the technology side of the FCC."[53]

Powell's focus at the FCC was to move the agency away from what he liked to call the one-wire problem. As he saw it, for decades telephone service was provided by a single, integrated monopoly--Bell Telephone--whose services had to be regulated to avoid price gouging. In exchange for the grant of that monopoly, the company was obligated to provide certain social goods, like making sure that everyone had a telephone connection and agreeing to serve everyone on reasonable and nondiscriminatory terms.

This was the right approach when there was only "one wire" going into each home. But Powell believed that other technologies, such as cable and perhaps wireless, would become viable competitors to the telephone, creating the possibility of multiple wires competing to provide a range of services. The problem, he thought, was that the regulatory structure had not yet adapted to this new reality.[54]

Powell's view, which he shared with many conservative economists in the early 2000s, was that when it came to Internet access, competition was not defined as different companies with the same technology vying for customers. Rather, different media--cable, wireless, satellite, and possibly "broadband over powerline" (using electrical connections to send data transmissions)--would compete, thereby providing the constraints on monopoly power that had once been imposed by regulatory structures. Instead of having the government force the key incumbent distribution network--before 1996, the telephone network--to make its poles and lines available to competitors providing Internet access, the distributors (now including wireless and cable as well as phone companies) would compete with one another to serve consumers. The result: protection for consumers against abusive pricing and monopoly-quality service without heavy-handed government regulation.

Powell's goal, then, was to facilitate the creation of multiple communications companies and technologies that would be able to reach homes and provide high-speed access to the Internet. Even a company with a monopoly over, say, cable would still have to compete with telephone and other companies. The existence of multiple deregulated platforms would drive down the price of connectivity and unleash innovation.[55]

In the long run, Powell's prediction proved wrong. Cable's advantages eventually became unbeatable: 90 percent of new wired Internet access subscriptions now go to the local cable incumbent, not the phone company, while wireless access is an entirely separate market.[56] But for a few years in the early 2000s, things worked out as he had anticipated: cable systems offered high-speed Internet access and made a few of their channels available for two-way transmissions running over the same hybrid coaxial fiber that brought the cable content into the home: cable-modem service. The development of the cable-modem service in turn drove the phone companies to improve their version of Internet access service over their metal lines: digital subscriber lines, or DSL. These services were clear competitors, at least initially, as they gave consumers access to the Internet at roughly similar speeds.[57]

This is where the problems began. The different modalities raised a regulatory conundrum: was high-speed Internet access via cable analogous to high-speed Internet over the phone, and therefore in need of the same common-carriage regulations? Or was it something new that should be left unregulated? Powell had another problem in creating a level playing field: if the two services were functionally indistinguishable, why should they be regulated in different ways?

The cable companies were confident they had the answer. Cable had never been regulated as a common-carriage service in the past; phone had been. It would stifle innovation, cable operators claimed, to treat cable-modem Internet access as a common-carriage system, even if the services provided were functionally the same as those of phone companies.[58]

Powell is by nature a free-market advocate, and he was frustrated by the weight of federal common-carriage regulation under Title II of the 1996 Telecommunications Act. He could not imagine why access to the Internet should be hampered by outmoded regulation. He would point out to anyone who would listen that the 1996 act took as gospel a model in which

the technology of any infrastructure is understood to be integrated with the use made of the technology: if a company is running copper wires and providing voice services, for example, it falls under Title II of the 1996 act and is regulated as a common carrier; if it is running coaxial fiber wires and providing entertainment, it is a cable service and falls under Title VI; if it is a broadcaster using the airwaves, it falls under Title III. He felt these distinctions were fine for old technologies. But they made no sense from a regulatory perspective when it came to Internet access. "When AT&T provides voice, video, and data over the same set of wires," Powell said, "you have a mess on your hands."[59]

Powell believed that when it came to high-speed Internet access via cable modems, he had a choice. He could take the existing Title II common-carriage requirements (nondiscrimination, sharing of connections) and "forbear" from--refuse to enforce heavily--the most onerous requirements, until only the portion of the regulation appropriate for high-speed Internet access was left. Or he could decide what social policies were truly needed (emergency service availability via 911 functionality, assistance to law enforcement) and apply regulations concerning them to high-speed Internet access one by one. As a free-market advocate, he was much happier "regulating up," starting with a blank, unregulated slate, than "deregulating down," starting with the multiple requirements of Title II. "Deregulating down" would require hundreds of pages of "forbearance" findings, a process he found distasteful and wasteful.

Powell had to act: cable-modem Internet access service was already in use, but it was in regulatory limbo. There had been a tussle since 1998 over how to treat it, but by the end of 2001 the Federal Communications Commission had not expressed a view except through one-off assertions in merger reviews. Powell's approach to this question set the United States on the road toward the titanic battles of 2010. Thanks to his bottom-up approach, the essential communications network of our time, access to the Internet, has no basic regulatory oversight at all.

The history of communications regulation in the late-twentieth and twenty-first centuries depended on one basic distinction: regulators have traditionally treated the transport of communications as a common-carriage service--open to all, subject to oversight to prevent discrimination, and bound by requirements to connect to other networks. Everything else, including data-processing services, was treated as a non-common-carrier "information service." When computers came into use in the 1960s and 1970s, the FCC was careful to draw a line between computer processing (information service) and the transport of data by the carriers (common-carriage service). The FCC did this as a regulatory matter to avoid giving the carriers power, in their gatekeeping role, over data processing. It would have been easy for the carriers to cross-subsidize and dominate data-processing businesses with their monopoly profits, and the FCC was trying to prevent that; it also wanted to avoid burdening the new computer services with the heavy superstructure of common-carriage regulation--rate-making, tariffs, and so on. Carriers were therefore prohibited from offering computing services. They were eventually (in 1980) allowed into this business, but only if they sold their basic transport services separately and without discrimination. The assumption was that carriers would keep selling basic transport under common-carriage rules.[60]

The 1984 AT&T divestiture was, in turn, designed to ensure that local phone companies would not be allowed to leverage their provision of local service into control over long distance. Under the supervision of Judge Greene, AT&T agreed to sell its Bell operating companies, which in turn agreed not to sell long-distance services, sell or manufacture telephone equipment, or--most important--get into the data-processing business. Then, in 1993, the restrictions on the RBOCs on providing data-processing services (or information services, as we now call them) ended (over Judge Greene's strong objections). This was a big victory for the carriers, and they wanted to cement it into statute. Shortly thereafter, drafting began on the 1996 act, which was aimed at removing communications-policy jurisdiction from Judge Greene's courtroom altogether and moving it to the expert agency--the FCC--while leaving in place the FCC

definitions that had separated data processing from common-carriage transport during the proceedings in the 1970s and 1980s.[61]

From 2000 to 2002, as Powell considered how to classify cable-modem Internet access services--which seemed to have characteristics of both DSL services and traditional cable services--the courts went ahead without him. The Ninth Circuit Court of Appeals decided that cable-modem services were indeed "telecommunications service" providers under the act and so were required to not discriminate and to interconnect; in other words, they were common carriers, similar to the old telephone companies.[62]

The FCC then declared--after the court had already spoken--that cable-modem service was an information service.[63] A data-processing service. This meant it would not be regulated. The FCC asked the Department of Justice to appeal the Ninth Circuit Court's decision, hoping to get the ruling reversed, which led to a Supreme Court decision during the summer of 2005, the Brand X case. As a legal matter, the FCC took the view that the Commission had been handed an ambiguous statute and had done its best to interpret it; the FCC should not be obligated to apply common-carriage principles to all possible carriers, even those the public viewed as providing general-purpose communications-transport services.

The Supreme Court deferred to the FCC's interpretations of "information service" and "telecommunications," as well as its deregulatory application of those interpretations to high-speed Internet access, overruling the Ninth Circuit Court's inconvenient opinion to the contrary. (This conclusion frustrated Justice Scalia, who issued a stinging dissent, possibly informed by his service as staff to the White House Office of Telecommunications Policy during the Nixon era. He contended that transmission is transmission and that it can be seen as separate from everything else.)[64] Shortly thereafter, the FCC declared DSL Internet access service an information service, leaving DSL providers (like cable-modem providers) free to act as they pleased, even to discriminate in pricing and access. Only voice communications over copper telephone wires were still subject to common-carriage obligations--and those services were rapidly losing their popularity.[65] The upshot was that all high-speed Internet access service was completely deregulated.

This move created a risk that the carriers would be able to price discriminate--choosing which online services to prioritize based on, say, their affiliation with the service. Carriers could thus ensure that people who wanted to pay more for particular content were able to do so ("capture consumer surplus")--which, from the carriers' perspective, would facilitate investment in additional high-speed Internet access facilities around the country. But consumer advocates worried that price discrimination and prioritization could mean that the carriers would be able to decide which uses of their networks were permitted--a power that could inhibit innovation, economic growth, and competition generally. Incumbents always want to block competitors. From the advocates' perspective, the Powell Commission's regulatory gymnastics served the interests of the enormous incumbent network providers by shielding them from traditional common-carrier obligations that would have allowed upstart businesses to thrive.[66]

To mollify its critics, during the summer of 2005 the FCC issued an Internet Policy Statement that outlined "four freedoms" for Internet users: access to content, access to applications, choice of devices, and competition among service providers.[67] But two of the commissioners deemed this statement unenforceable, and the policy statement itself was subject to "reasonable network management" and the "needs of law enforcement"--unclear concepts at best.[68] Given these caveats and the lack of clarity surrounding the policy's legal status, it is not surprising that people who were already worried about the future of the open Internet were not satisfied.[69]

The "net neutrality" fights that followed Powell's deregulation of high-speed Internet access were fierce and included several prolonged and painful attempts to pass and defeat legislation. But the most important thing that happened next was a discovery by an Associated Press reporter and the Electronic Frontier Foundation (EFF).

<ls>

During the fall of 2007, many Comcast users began to notice that their ability to share digital files over BitTorrent, an Internet protocol that allows people to share digital files without hosting or streaming the entire file, had been compromised. Most blamed their own computers, or the weather, or a number of other elements. Few guessed that their network access provider was blocking their ability to share video files--even if such a thing were possible, it would not have seemed right. But Robb Topolski, a barbershop-quartet enthusiast (and Intel engineer), and researchers at EFF decided to check out the disruptions more systematically.

BitTorrent works by cutting large files into pieces and allowing other users (peers) to make those pieces available across transport networks, enabling even users of devices with limited bandwidth (such as early mobile phones) to share large data files, like video. The process results in servers being contacted hundreds of times a second, a detail that Topolski and the EFF thought might provide an opportunity for someone to interfere. Independently setting up controlled experiments and trying to download a copy of the King James Bible and other non-copyrighted works, Topolski and the EFF discovered that Comcast was effectively telling both sides of a BitTorrent communication, "Sorry, I have to hang up now," and forcing the communication to terminate. Comcast was "hanging up" on attempts to use the BitTorrent protocol.[70]

When Topolski's story was published in the Associated Press, it had a sensational impact.[71] Net neutrality supporters had long suspected such corporate interference, and here was their smoking gun--and, in fact, the gun was still being fired every day. Comcast was throttling BitTorrent video traffic that conspiracy-minded technologists thought might be competing with Comcast's own video plans.

Kevin Martin, then the chairman of the FCC, was known for his relentless pressure on the cable industry. He went after Comcast during two public hearings that further added to the uproar.[72] (Martin has become known in telecom circles more for his Machiavellian political hijinks than for his policies. This reputation doesn't do him justice; he clearly took action vis-à-vis the cable industry.) At the end of the summer of 2008, Martin announced that Comcast's practices amounted to unreasonable network management under the FCC's 2005 Internet Policy Statement. The Commission imposed no injunction or fine but insisted that Comcast promise to adopt a protocol-agnostic method of network management by the end of 2008.[73]

Comcast could have let matters stand; the Commission would have continued muddling along under its assumption that it could regulate high-speed Internet access providers (to some extent, at least) under the non-common-carriage Title I of the Telecommunications Act and its dubious Internet Policy Statement. But Comcast was bothered by having to account to the Commission for its network-management practices--to Comcast, the FCC's action appeared to be ad hoc, unprincipled, and based on little more authority than its assertion that the Commission was in charge. Comcast sued, and in April 2010 it won.[74]

The D.C. Circuit Court of Appeals found that there was nothing in the 1996 act to which the FCC's Comcast adjudication was "reasonably ancillary." Congress simply had not delegated power to the FCC to regulate network-access providers that the Commission had already labeled as deregulated. That label, it turned out, made a major difference. Powell's desire to "regulate up" (starting from scratch) rather than "regulate down" (by classifying these services as Title II and then restraining the Commission from applying rate regulation and other old-fashioned rules) had proven to be unenforceable; the D.C. Circuit Court ruled that the Commission had no delegated power over Comcast's behavior after it had expressly declined to regulate in this area. The FCC suddenly found itself to be a regulator with no clear regulatory authority over the central communications medium of the age: Internet access.

In short, the Commission had taken the basic idea in the Telecommunications Act--that general-purpose two-way networks should be labeled common carriers, obliged to treat

everyone equally--and, with no direction from Congress, had relabeled high-speed Internet access as . . . something else.

The months following the decision were a frenzy of attacks and counterattacks. A difficult question confronted the FCC: could it continue to label high-speed Internet access a "deregulated" service and still accomplish its regulatory goals of achieving ubiquity, neutrality (an Obama campaign promise), and other policy ends? Or would it have to reclassify high-speed Internet access service as a "regulated" service (a Title II service) in order to tell providers what to do?

The new FCC chairman under President Obama, Julius Genachowski, was in an uncomfortable position. Since the deregulatory decisions in the mid-2000s by Michael Powell's FCC, cable companies had invested billions of dollars installing high-speed Internet access infrastructure and related facilities. Pointing out that 93 percent of the country was now reached by cable infrastructure,[75] the cable trade association argued that changing the rules governing how network access was regulated would stifle their ability to attract investment that could be used to serve difficult-to-reach areas.[76]

Genachowski is not a bomb thrower. He has an eager way of speaking and a lawyerly, precise mind. He had served on the Harvard Law Review with President Obama and wanted to avoid embarrassing the president; he also wanted to be seen as a business-friendly, investment-conscious centrist. Genachowski had been sworn in at the end of June 2009, and the first several months of his tenure had been occupied with creating the National Broadband Plan called for by the stimulus bill enacted at the beginning of the Obama administration. He had assembled a huge team to research and draft the plan, which was delivered in March 2010. The plan did not propose deep changes in America's broadband structure or make any substantive effort to deal with concentration in the market for Internet access. It did note that there would be a strong cable monopoly for video-speed broadband by 2015--a reasonable point, given that only cable would be sufficiently upgraded to allow for speeds beyond 50 Mbps, that the phone companies were reluctant to make the necessary investments to lay fiber, and that there would be no competition among cable providers--and it suggested that municipalities should be able to bring high-speed Internet infrastructure to their citizens. The report also suggested a lengthy transition in which the government would switch to subsidizing high-speed Internet access rather than telephone service (so-called "universal service").[77]

At the same time, the Commission had run a separate rulemaking process aimed at the president's apparent campaign commitment to address net neutrality. Hoping to keep the National Broadband Plan uncontroversial, the Commission carefully kept net neutrality out of it.

But after the D.C. Circuit Court opinion in the BitTorrent case in April 2010, that separation became untenable. The court had ruled that the FCC did not have the power to make Comcast ensure that its "network management" was reasonable--and the arguments the Commission had used to support its exercise of authority over Comcast in the BitTorrent case were the same ones supporting its net neutrality arguments. Using the same legal tactics to support net neutrality would, it seemed, run up against problems with the D.C. Circuit Court. Similarly, the FCC's "universal service" policies in the National Broadband Plan were threatened--only a Title II common-carriage service could be subsidized and high-speed Internet access now fell under Title I. The same labeling that had released high-speed Internet access from regulatory obligations meant that federal subsidies could not be provided to allow Internet access for everyone.

The FCC had hoped to keep the court focused on process, not on the substance of its authority, and both Genachowski and his lawyers were surprised by the outcome of the Comcast case. All other work stopped at the Commission as the FCC considered legal options. Genachowski and his lieutenants did not want to spark a war with the carriers. But they were deeply worried that everything they tried to do would be the subject of prolonged and painful litigation--every step would be examined to see whether it was "reasonably ancillary" to the

exercise of the Commission's authorities under the Telecommunications Act, and the FCC would never be able to get anything done. The situation was a mess. And it was about to get worse.

On Monday, May 3, 2010, the Washington Post reported that Genachowski had decided not to reclassify high-speed Internet access as a Title II service in the net neutrality proceeding.[78] The incumbent carriers, including Comcast, must have been delighted; this is what they had been fighting for. Then, three days later, the chairman's office issued a press release. The FCC was going to suggest reclassification after all, but would restrain itself--forbear--from carrying out many of the traditional elements of common-carriage regulation under Title II.[79] A predictable firestorm of lobbying and complaints arose from AT&T and the other incumbents. How could there be a move toward regulation? Analysts called the FCC's move the "nuclear option." The rhetoric rose higher: Genachowski, the carriers said, was trying to destroy the communications industry. Even the hint of reclassification was too much for the industry to accept.[80]

The pressure on the chairman to change his position was intense: AT&T spent almost six million dollars in the first quarter of 2010 alone lobbying the Commission, the Department of Commerce, the White House, and anyone else its lawyers could think of to convince them that the FCC was planning to "regulate the Internet."[81] The company marched on the Hill, getting signatures from 171 House Republicans and 74 House Democrats for letters excoriating Genachowski for considering reclassification of the transport portion of Internet access services.[82] The campaign was reminiscent of John D. Rockefeller's attack on Theodore Roosevelt in 1907, when he proclaimed that Roosevelt's antitrust policies would bring "disaster to the country, financial depression, and chaos."[83]

Eventually the chairman changed his mind once again: in a follow-up document, he suggested that reclassification was just one of many options on the table. One of the other options, he said, was for the Commission to continue as it had been doing--relying on authority based on "ancillary jurisdiction"--the idea that whatever the FCC was doing would support one of its express statutory delegations. Rather than stating which way the Commission intended to go, the follow-up statement presented all options; everything was still on the table. A long, hot summer of lobbying lay ahead.[84]

The FCC started holding off-the-record stakeholder meetings to explore whether a deal was possible that would preserve an open Internet without strangling the carriers' ability to attract investment. Congress began its own series of closed-door sessions. The world of telecom policy seethed with rumors and discontent. In the end, after months of wrangling, the FCC agreed with the carriers in late December 2010 that they would keep their Title I classification.[85] Within this framework, the Commission applied a very light hand to wired providers of Internet access, embracing usage-based billing and the idea of "managed services" that would not be subject to neutrality requirements. Wireless providers were freed of any obligation to refrain from discriminating against online applications. For Comcast, this was good news: it could continue its vertical integration plans without having to worry (for the moment, at least) about governmental review of its control over its pipe to American homes. Verizon sued. Someone always sues.

<ls>

Over several decades, the U.S. government has tried--not always successfully--to force incumbents to let new competitors have access to the materials they need to compete. Where incumbents act as gatekeepers, new technology will not emerge without regulatory help that creates a level playing field for competition and the free flow of information. The government did this for the cable industry in the late 1970s when it mandated pole-attachment sharing, for the computing industry in the 1970s and 1980s when it protected the new industry from the depredations of the telephone monopoly, for long-distance service in the mid-1980s with the AT&T divestiture, for the nascent satellite industry in the early 1990s through program-access

rules in the 1992 Cable Act, and for high-speed Internet access in the late 1990s through common-carriage rules for DSL.

Incumbents will also use all available regulatory levers to protect their business models: the broadcast industry used FCC's broad statutory power to fend off competition from cable in the 1970s; the cable industry used vague program-access rules to make life more expensive for smaller cable providers and satellite companies in the 1990s and 2000s; and the telephone companies used vague language in the 1996 Telecommunications Act to fight attempts to force them to share their local facilities.

Behavioral restrictions are difficult to enforce; structural limitations such as the separation of carriers from content are difficult to achieve politically. The pendulum swings back and forth: cable deregulation in 1984 was followed by reregulation in 1992; the structural separation signaled by Al Gore and feared by John Malone was never carried out, and vertical integration has become common and unquestioned. Genachowski's FCC was apparently not interested in diverging from Michael Powell's view that consumers and innovation would be adequately protected by the market--and that traditional regulation was not necessary.

LAW & DISORDER / CIVILIZATION & DISCONTENTS

US net neutrality rules finalized, in effect November 20

The FCC passed weak net neutrality rules last December, but they won't be ...

by Nate Anderson - Sept 22 2011, 3:41pm EDT

63

Get ready, America—net neutrality finally comes to the Internet on November 20, 2011.

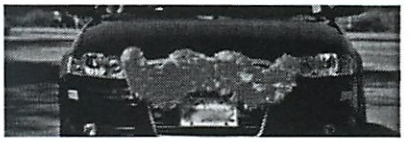
That's the plan, at least. The FCC has just filed its final "open Internet" rules (PDF) with the *Federal Register*, which will publish them tomorrow and make them official. The rules go into effect on November 20, nearly a year after they were passed over Republican opposition on a 3-2 vote. (One of the FCC Commissioners who voted against the rules now works for Comcast.)

But the plan will likely be derailed by lawsuits. Two, by Verizon and MetroPCS, were filed earlier this year but tossed because the rules had yet to be finalized. With tomorrow's printing in the *Federal Register*, the litigation floodgates will be thrown open and and complaints about the government overstepping its authority can start pouring in.

Those complaints might well meet with success, given how the FCC went about the whole process. Rather than reclassifying broadband services in such a way that the FCC has clear jurisdiction over them, the agency relied instead on its much weaker "ancillary jurisdiction." (The legal rationale for this begins on p. 77 of the final rules, and the FCC gamely makes a case that it has the proper authority.) As law professor James Grimmelmann noted today in our subscriber-only webchat, "The FCC is in a real tangle here. I think if they reclassified broadband service (long story), they'd have a better shot at getting their rules to stick."

As for the rules, they're the same modest regulations adopted back in December. Here's the FCC's own summary:

TOP FEATURE STORY



FEATURE STORY (2 PAGES)

Transportation innovation: How Lyft and SideCar are changing commuting

Smartphone apps + "ride-sharing" = travel revolution? Two startups say yes.

107

STAY IN THE KNOW WITH

LATEST NEWS

A rare tour of the Stanford Linear Accelerator Center (in pictures)

Demolishing Heisenberg with clever math and experiments

GAMING & ENTERTAINMENT

Unreal Tournament bots appear more human than humans

EXCESSIVE FORCE

Cop accused of tackling 15-year-old in retaliation for videotaping

INFINITE LOOP / THE APPLE ECOSYSTEM

AT&T defends FaceTime decision: "There is no net neutrality violation"

The carrier says consumer groups had "another knee-jerk reaction."

by Jacqui Cheng - Aug 22 2012, 11:[illegible] EDT

GOVERNMENT IOS & IDEVICES MOBILE COMPUTING 126

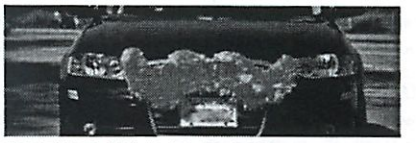
AT&T is defending its decision to limit the use of Apple's video chat feature, FaceTime, to its Mobile Share data plans by saying that the limitation does *not* violate the FCC's net neutrality rules. The company wrote in a blog post on Wednesday that some groups had "another knee-jerk reaction" to AT&T's limitation, but the company argues that its decision meets all FCC requirements.

Last Friday, AT&T issued a statement confirming that the carrier wouldn't charge extra for the use of FaceTime over 3G like many had suspected. However, the company *did* say that customers who want to use the iPhone video chat feature would be required to subscribe to one of AT&T's new Mobile Share data plans—AT&T's version of a shared data pool that can be used across multiple devices.

The catch for users is two-fold. When we covered AT&T's plans in July, we noted that the savings were not particularly great for many users, particularly the solo tablet-and-smartphone user. As such, it doesn't make much sense for those users to pay extra for a different plan just so they can use FaceTime. More importantly, switching over to the Mobile Share data plan would force many data users who are currently subscribing to grandfathered data plans to give up their unlimited data. AT&T has long said that it would allow unlimited data subscribers to continue using their plans (which are no longer offered to new customers) as long as they didn't change their subscriptions, but those users won't be able to use FaceTime over their cellular connection unless they make that change.

And that's just the beginning. A number of consumer groups immediately reacted to the announcement by saying AT&T's decision violated FCC's Open Internet rules by placing a limitation on the video calling feature. "These rules state that mobile providers shall not 'block applications that compete with the provider's voice or video telephony services.' Although carriers are permitted to engage in 'reasonable network management,' there is no technical reason why one data plan should be able to access

TOP FEATURE STORY



FEATURE STORY (2 PAGES)

Transportation innovation: How Lyft and SideCar are changing commuting

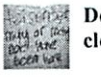
Smartphone apps + "ride-sharing" = travel revolution? Two startups say yes.

107

STAY IN THE KNOW WITH

LATEST NEWS

A rare tour of the Stanford Linear Accelerator Center (in pictures)



Demolishing Heisenberg with clever math and experiments

GAMING & ENTERTAINMENT

Unreal Tournament bots appear more human than humans

EXCESSIVE FORCE

Cop accused of tackling 15-year-old in retaliation for videotaping

Inside NZ Police Megaupload files: US investigation began in 2010

FCC to buy out TV broadcasters to free up mobile spectrum

statement.

But AT&T argues that's not the case at all, because the FCC only requires service providers to be transparent about their network management practices, and prohibits providers from blocking applications that compete with the provider's voice or telephony services.

"AT&T's plans for FaceTime will not violate either requirement. Our policies regarding FaceTime will be fully transparent to all consumers, and no one has argued to the contrary. There is no transparency issue here," AT&T Senior VP of Regulations Bob Quinn wrote on Wednesday.

"Nor is there a blocking issue," Quinn continued. "The FCC's net neutrality rules do not regulate the availability to customers of applications that are preloaded on phones. Indeed, the rules do not require that providers make available any preloaded apps. Rather, they address whether customers are able to download apps that compete with our voice or video telephony services. AT&T does not restrict customers from downloading any such lawful applications, and there are several video chat apps available in the various app stores serving particular operating systems. (I won't name any of them for fear that I will be accused by these same groups of discriminating in favor of those apps. But just go to your app store on your device and type 'video chat.') Therefore, there is no net neutrality violation."

AT&T argues that customers have always used and may continue to use FaceTime over WiFi without restriction—the company is just *broadening* customers' ability to use FaceTime by allowing its use over the Mobile Share data plans.

But the company's arguments aren't likely to make consumers *or* consumer groups feel any better. In an e-mailed statement on Wednesday morning, Free Press research director S. Derek Turner argued that AT&T's defense doesn't hold up.

"AT&T is inventing words that are not in the FCC's rules in a weak attempt to justify its blocking of FaceTime," Turner said. "There is simply nothing in the rules that distinguishes 'preloaded' applications from 'downloaded' applications. It is interesting to see AT&T try this line of defense, as it is tacitly admitting that it is both blocking FaceTime and that the app does in fact compete with its own offerings. FaceTime allows people to reduce their use of voice services, but AT&T is making you buy unlimited voice in order to use FaceTime over mobile. AT&T is trying to invent a loophole in the rules, but this kind of anti-consumer behavior is the exact thing the FCC's protections are designed to prohibit."

Public Knowledge also issued a new response to AT&T's statement. "The FCC's Open Internet rules do not distinguish between pre-loaded and downloaded apps. They prevent carriers from blocking certain kinds of apps--period. AT&T is blocking FaceTime for all of its iPhone customers who do not subscribe to its premium 'Mobile Shared' plans, and this runs afoul of the rules," Bergmayer wrote on Wednesday.

Free Press is currently running a petition to stop AT&T's "latest attack on net neutrality."

READER COMMENTS 126

Jacqui Cheng / Jacqui is senior Apple editor at Ars Technica, where she has spent the last seven years writing about Apple culture, gadgets, social networking, privacy, and more.

Follow @eJacqui

← OLDER STORY NEWER STORY →

YOU MAY ALSO LIKE

STS. 805
Net Neutrality

10/4

(fewer students)

Have not talked about network layers

Today: NN Normative pov

Exec branch rule making

Open Internet Order

Cold calling:

Madison River Telco

blocked Vonage

Ok:

if transparent: then ok:

if monopoly:

if competition: then ok:

4 6,000 + dial up isps

6

(2)

Monopoly leveging

do you need a phone?

how is Apple different?

natural monopoly?

buy vs use service

Cons → why are picking on a particular network

Why is [redacted] ok for Google to return Google Maps at the top

Classic antitrust market?

[redacted] or is there something else?

network providers vs edge providers

Something special about speech?

(I forgot all these issues ...)

(3)

(or prof is not agreeing)

1st Amendment does not apply to AT+T
only to gov

Something Special about Speech + com system

Opposes spirit of free market

Vince Cerf: innovation > permission
how many needed to be competitive?

Why not

my CDN example
(went over his head)

pay for extra guarentee
barrier to entry
"like a mafia"

(4)

Six Flags charges extra for front of line

Common Carriage - treat all calls the same

Wireless vs wired?
make a difference?

specialized service

incentivizing investment

Special deal → when they pay for data
network management

What do you do about?

Why can it create a rule?

Congress can regulate ~~congress~~ interstate commerce

Congress created FCC

(5)

How agencies make rules?

"The regulatory state"

Should you regulate?

Congress delegates authority to regulatory authority

FAA → air planes

FCC → tekcom

etc

FCC, FTC ind. agency

President can't really control

Rulemaking proces

1. Notice of Inquery
   Public comments
2. Notice of Proposed Rulmaking
   - Draft

(6)

Elaborate commenting round

lots of pape

So rulemaking proces is open + trasparent

Must explain thinking when making rules

Administrative Procedre Act

very boring

but very important

done by non-elected

Carrer staff

Supervised by ~~[illegible]~~ politically appointed person

3. Final Rule

4. Lawsuit

- unconstitutional
- arbitray + capricous
- ~~not~~ no authority
- rules not followed
- etc

(7)

- adq relationship b/w facts + rules

- can take a while

- New childrens rules
  - Statue 1988
  - 1st rules 2000
  - revised last week
    but now all sorts of fuss

Is this process nimble enough

Or industry self regulate

Lots of filing
tens of thousands of $ on lawyer fees

big cos follow rules
protect brand
huge fines

(8)

Three prong rule

- transparency
- non discriminate
- no blocking

Wireless different ...

Telecommunications vs info services

how to apply the rules?

does the FCC even have the authority to act?

Lawsuit

maneuvering to get into DC circuit

which likes carriers

betting if is rules will be thrown out

Congress could pass law

FCC could reclassify

but would be arbitrary + capricious

Currently in force for broadband providers

(9)

Verizon filing early
totally deliberate
aggressive
race to Carthage to be in right venue
who is friendly

David Clark

Chairman of IAB
Co-author of end to end argument
Technologists not in charge

Thinks FCC guided into the corner
Computer 1 and 2
FCC wanted to forebare internet regulation
BA must now live w/

Europe - can regulate internet
Asia - no one challenges regulator

(10)

Net Neutrality

1. User experience
   - not neutral, never has been
   - 80s were prioritizing remote log in traffic
   - Competing w/ TCP
   - really not true
   - w/ goal to improve cust exp

2. ISPs need $, but not enough
   - read Comcast's anual report
   - 10-11% margin
   - Why worried about them making $
   - Do they grow?
     - Return on investment?
       - not hard to tell
       - it sucks

(11) Why ever upgrade?

World have to ↑ capacity 50x
to support over the top video

Peering + transit

10/8

6.805 Semester Project Proposal

Michael E Plasmeier <theplaz@mit.edu>
Stephen J Suen <ssuen@mit.edu>

2012 saw the reemergence of copyright legislation in the public consciousness, especially in the wake of SOPA and PIPA, which sought to combat piracy on the Internet. The resulting backlash against these bills—both from Internet users and businesses themselves, as well as from political opposition—indicate divisive attitudes over the effectiveness of the proposed anti-piracy mechanisms. Our project aims to analyze the major policy proposals targeting online piracy. We will not only be looking at the mechanisms put forward in SOPA, PIPA, and proposed alternative OPEN, but we will also review the success of policies implemented via the DMCA and through voluntary action by Internet players. Where appropriate, we will evaluate policies implemented around the world such as the French Hadopi law, unilateral policies including Hollywood's monitoring of BitTorrent networks, and provisions included in international treaties like ACTA. The specific policy mechanisms that we will review are:

- Requiring US-based DNS providers to alter results
- ISP-based deep packet inspection
- BitTorrent monitoring
- Copyright infingement lawsuits against individual users
- DMCA takedown requests
- Legal action against upload sites (e.g. Megaupload)
- Content identification by video sharing websites (e.g. YouTube Content ID)
- Graduated response (e.g. Hadopi in France, voluntary 6-strikes agreement in the US)
- Stopping advertising revenues
- Criminal penalties
- Preventing distribution/discussion of circumvention tools
- *Possibly others, pending additional research*

Naturally, to evaluate the piracy-fighting effectiveness of each of these mechanisms, we will design a model of cost-benefit analysis that incorporates various assessment metrics. For each proposed mechanism, we will pose a number of questions. Will the policy actually make a difference? Can the policy be implemented robustly? Can pirates easily avoid the mechanism? What are the costs and challenges of implementation? Does the policy violate the standards of the Internet? Will the policy prevent us from accomplishing other goals, such as tightening up cyber security? Will certain actors incur a cost, and if so, who will pay for it? To supplement this analysis, we will review existing literature on the economic costs of online piracy and develop a system of classifying these losses.

Based on these issues, the goal of this report will be to identify possible policy actions that address the piracy problem without compromising the underlying structures of the open Internet and—by extension—the civil liberties guaranteed by those structures and the ecosystem for innovation that they have enabled. This analysis will also take into account pragmatic issues of economic costs, possible political challenges, and other barriers to comprehensive implementation. We will also be sure to examine copyright law pre- and post-Internet, to see how notions of intellectual property and proper enforcement of those exclusive rights have changed over time, in order to better contextualize the issues at play.

A-

Net Neutrality Memo

Michael Plasmeier[1]

To: John "Jay" Rockefeller (D-W.Va.)

Net neutrality is a term used to describe various rules or proposed rules that would restrict Internet Service Providers (ISPs) and other owners of IP-based networks considered to be part of the public Internet from blocking, restricting, or otherwise degrading the traffic which travels over those networks.

Proponents

Internet Companies: Google, Amazon, Free Press, Public Knowledge, Larry Lessig

Opponents

Big ISPs: AT&T, Comcast, Verizon

Arguments for net neutrality

- Protect freedom of expression online
- Allows upstart companies to compete; equal playing field
- Prevents ISPs from charging both ends of the network; seeking additional rents
- "Reasonable network management practices" still allowed
- ISPs form a duopoly in most regions
- Otherwise ISPs would favor their own vertically interested services

Arguments against net neutrality:

- Peering and transit contracts have always been privately negotiated/unregulated
- May prevent new IP multicast solutions which could make it easier to stream video online
- May prevent CDNs from paying to be deployed deep within an ISPs network, slowing internet traffic and adding a greater burden of overall traffic
- No current market failure
- Would disincentives investment in additional broadband
- Is an uncompensated taking

In 2011, the FCC issued its final report and order codifying net neutrality. The FCC has been writing rules on net neutrality since its initial 4 freedoms policy statement in 2006. The rules were written with the inclusion of industry over the last several years.

The FCC issued the rules under its Title 1 ancillary authority to regulate information services. The distinction originally comes from when you used a phone in a special cradle to call a specific service (like LexisNexis). When you wanted to reach a different service, you would hang up and dial that service. The phone call was a *telecommunications service* like normal, while the service you called was an

[1]This paper contains content from my group report on Net Neutrality for STS.011 for Fall 2011 http://minisites.theplaz.com/netneutrality/

Comment [DNSU1]:
Grade: A-

Dear Michael,

The writing here is really excellent throughout and you are admirably clear and complete.

As a matter of format, this is a bit off. It reads like a very good briefing paper, not a memo.

I've highlighted two paragraphs (near the bottom) that really belong right up top (1 and 2).

For a memo you want (instantly): Here's the main message; here's what we should do.

You follow a very logical and well developed process and build the context for us. That's great, but you backfill with that in a memo (you assume many people will only read the first paragraph).

Best,
Don

information service. Soon information services grew to include ISPs which allowed you to visit any site on the network of services called the Internet. There were 1000s of dial up ISPs of which you could call any of them with your phone. When DSL came out, which used unused frequencies of the phone line, the FCC required that phone companies lease the lines to upstart companies, as part of deregulation. However, cable internet, and now fiber internet access has always been seen as an information service and has been by-and-large unregulated.

Recent Court Case

Verizon sued to prevent the net neutrality rules from being applied, arguing the FCC did not have the authority to issue these rules. The Court ruled today that the FCC does not have the authority under Title I to pass these rules.

Comment [DNSU2]: This is your intro paragraph (with some details filled in: On [Date] DC circuit, ruling in [Foo vs. Smith]. . .

Moving Forward

Reclassification

Moving forward, the FCC can choose to reclassify broadband internet from an *information service* to a *telecommunications service*. This would give the FCC clear authority to impose the rules, but it would also bring all of the other Title II rules (such as *common carriage* and *open access*) to broadband internet access. In addition, many think the courts would strike down this reclassification as capricious because it is contrary to the regulatory history of the FCC over the last 20 years.

Congress's Role

Congress could also pass a law giving the FCC explicit authority to impose net neutrality rules. This is likely the best option, as it would allow the FCC to cleanly ensure net neutrality happens and to not saddle the Internet with unnecessary regulation. In fact, you could use this argument to try to persuade your GOP colleagues – that this would preserve freedom online while avoiding burdening the Internet in regulation.

Talking Points

- Net neutrality is important for freedom of speech online and to allow small businesses to compete
- We are disappointed the Court overturned net neutrality
- I will be working with my colleagues in the Senate to pass a law giving the FCC clear authority to pass these net neutrality rules
- We want to avoid the FCC adding more burdensome regulations to the Internet by reclassifying it as a Title II service

Comment [DNSU3]: Would make a good second paragraph/section.

6.805 Class 6, Oct. 11, 2012: Fourth Amendment Basics

Read 10/11

Class 6, Oct 11, 2012 - Fourth Amendment Basics

6.805: Foundations of Internet Policy - **Semester Calendar**
meets in 36-156

Goals

This week's class provides a grounding in Fourth Amendment jurisprudence, especially as it relates to wiretapping and other electronic surveillance.

Class Preparation

Fourth Amendment Foundations

Read the following court cases, one from old English law, and three seminal US Supreme Court cases. We are not asking you to write up briefs to turn in, but you might find it useful to brief these for yourself as a good way to prepare for class discussion.

- Semayne's Case. "A man's home is his castle" case from 1604.
- *Terry v. Ohio, 392 U.S. 1 (1968)* The "stop and frisk" case.

Oh were we supposed to do this before - didn't see it listed

Evolution of Fourth Amendment doctrine regarding electronic surveillance

- *Olmstead v. United States*, 277 U.S. 438 (1928). This was an early rejection by the Supreme Court of Fourth Amendment rights in telephone conversations, on the grounds that wiretaps do not constitute a physical search, and nothing is actually seized. Make sure to read the entire opinion, including Brandeis's dissent, which forms the basis of your writing assignment due for this week.
- *Katz v. United States*, 389 U.S. 347 (1967). This decision effectively reversed *Olmstead* and established a reasonable right of privacy in electronic communications, on the grounds that "the Fourth Amendment protects people, not places."
- House Judiciary Committee Report on the Electronic Communications Privacy Act of 1986, H. Rep. No. 99-647, 99th Cong. 2d Sess. 2 (1986) , especially pp. 16 - 27
- 18 USC 2703: Required disclosure of customer communications or records. Enacted as part of the 1986 Electronic Communications Privacy Act.
  - Digital Due Process Coalition memo on potential for reforming ECPA, The Electronic Communications Privacy Act of 1986: Principles for Reform, J. Beckwith Burr, (3/30/2010)

Opps Where is this listed?

Ask Hal

Agenda 2013 Activity

Each team should give a 3-minute talk presenting your plan for doing research, including a problem statement, writing, and schedule for meeting with your mentor. Each team should also describe how they

will divide up the work. One person on the team needs to be selected as the report editor and will have overall responsibility for the final product.

Assignment for Oct. 18

Next week's assignment is basically the same as this week's: Each team should give a 3-minute talk sayng where you are in your project, emphasizing the progress you made between Oct. 11 and Oct. 18, and highlighting how you've been working with your mentor. Don't be fooled by the lack of a written project assignment for Oct. 18. For Oct. 25, you'll need to turn in an outline of the paper that includes a very clear description of the problem you are addressing, with several possible solutions. So you should be able to describe some of that in your presentation for the 18t.

Where is this written thing described

~~f~~ing vague assignments!

Read 10/11

Semayne's Case

COURT OF KING'S BENCH

All ER Rep 62, Also reported 5 Co Rep 91 a; Cro Eliz 908; Moore KB 668; Yelv 29; 77 ER 194

Michaelmas Term, 1604

UK

JUDGMENT-1:
SIR EDWARD COKE:

In his report, said that the court resolved the following points: (i) That the house of everyone is to him as his castle and fortress, as well for his defence against injury and violence, as for his repose; and although the life of man is a thing precious and favoured in law so that, although a man kills another in his defence, or kills one per infortunium [by misfortune] without any intent, yet it is felony, and in such case he shall forfeit his goods and chattels [1]for the great regard which the law has to a man's life, but if thieves come to a man's house to rob him, or murder, and the owner or his servants kill any of the thieves in defence of himself and his house it is not felony, and he shall lose nothing, and therewith agree 3 Edw 3 Coron 303 and 305, and 26 LIB Ass pl 23.

So it is held in YB 21 Hen 7, fo 39, pl 50, everyone may assemble his friends and neighbours to defend his house against violence; but he cannot assemble them to go with him to the market or elsewhere for his safeguard against violence; and the reason of all this is because domus sua cuique est tutissimum refugium [his own house is the safest place of refuge].

[1] But see Offences Against the Person Act, 1861, s 7 (5 HALSBURY'S STATUTES (2nd Edn) 790) now repealed by the Criminal Law Act 1967, Sched 3, part 1.

(ii) That when any house is recovered by any real action or by ejectione firmae, the sheriff may break [into] the house and deliver the seisin or possession to the demandant or plaintiff for the words of the writ are habere facias seisinam, or possessionem, etc, and after judgment it is not the house in right and judgment of law of the tenant or defendant.

(iii) That in all cases when the King is party, the sheriff (if the doors be not open) may break [into] the party's house, either to arrest him or to do other execution of the King's process, if otherwise he cannot enter. But before be breaks [into] it, he ought to signify the cause of his coming and to make request to open the doors. That appears well by the Statute of Westminster the First (1275) c 17 [repealed]

(which is but an affirmance of the common law) as hereafter appears, for the law without a default in the owner abhors the destruction or breaking [into] of any house (which is for the habitation and safety of man) by which great damage and inconvenience might ensue to the party when no default is in him; for perhaps he did not know of the process of which, if he had notice, it is to be presumed that he would obey it.

That appears by the book in 18 Edw 2, Execut 252, where it is said that the King's officer who comes to do execution, etc, may open the doors which are shut, and break them, if he cannot have the keys; which proves that he ought first to demand them: YB 7 Edw 3, fo 16, pl 15 J beats R so as he is in danger of death, J flies, and thereupon hue and cry is made, J retreats into the house of T. They who pursue him, if the house be kept and defended with force (which proves that first request ought to be made) may lawfully break (into) the house of T, for it is at the King's suit: 27 LIB Ass pl 66. The King's bailiff may distrain for issues in a sanctuary: 27 (28) LIB Ass pl 35. By force of a capias on an indictment of trespass the sheriff may break [into] his house to arrest him; but in such case, if he breaks [into] the house when he may enter without breaking [into] it (that is, on request made, or if be may open the door without breaking [in]) he is a trespasser: 41 LIB Ass 15.

On issue joined on a traverse of an office in Chancery, venire facias was awarded returnable in the King's Bench without mentioning non omittas propter aliquam libertatem; yet forasmuch as the King is party, the writ of itself is non omittas propter aliquam libertatem; YB 9 Edw 4, 9. For felony or suspicion of felony the King's officer may break (into) the house to apprehend the felon, and that for two reasons: (a) for the commonwealth, for it is for the commonwealth to apprehend felons; (b) in every felony the King has interest, and where the King has interest the writ is nonomittas propter aliquam libertatem; and so the liberty or privilege of a house does not hold against the King.

(iv) That in all cases when the door is open, the sheriff may enter the house and do execution at the suit of any subject, either of the body or of the goods; and so may the lord in such case enter the house and distrain for his rent or service: YEAR BOOKS 38 Hen 6, 26 a; 8 Edw 2, Distr 21; and 33 Edw 3, Avow 256. The lord may distrain in the house although lands are also held in which he may distrain: vide 29 LIB Ass 49. But the great question in this case was if by force of a capias or fieri facias at the suit of the party, the sheriff, after request made to open the door and denial made, might break [into] the defendant's house to do execution if the door is not opened.

It was objected that the sheriff might well do it for divers causes:

(a) because it is by process of law; and it was said that it would be granted on the other side that a house is not a liberty, for if a fieri facias or a capias be awarded to the sheriff at the suit of a common person and he makes a mandate to the bailiff of a liberty who has return of writs who nullum dedit response, in that case another writ shall issue with non omittas propter aliquam libertatem.

Yet it will be said on the other side that he shall not break into the defendant's house as he shall do of another liberty, for whereas in the county of Suffolk there

are two liberties, one of St Edmund Bury and the other of St Etheldred of Ely, suppose a capias comes at the suit of A to the sheriff of Suffolk to arrest the body of B and the sheriff makes a mandate to the bailiff of the liberty of St Etheldred who makes no answer; in that case the plaintiff shall have a writ of non omittas, and by force thereof he may arrest the defendant within the liberty of Bury, although no default was in him;

(b) admitting it to be a liberty, the defendant himself shall never take advantage of a liberty; as if the bailiff of a liberty be defendant in any action, and process of capias or fieri facias comes to the sheriff against him, the sheriff shall execute the process against him, for a liberty is always for the benefit of a stranger to the action:

(c) for necessity the sheriff shall break (into) the defendant's house after such denial as is aforesaid, for at the common law a man should not have any execution for debt but only of the defendant's goods. Suppose, then, the defendant would keep all his goods in his house and so the defendant himself by his own act would prevent not only the plaintiff of his just and true debt, but there would also be a great imputation to the law that there should be so great a defect in it, that in such case the plaintiff by such shift without any default in him should be barred of his execution and the book in 18 Edw 2 Execut 252 was cited to prove it, where it is said that it is not lawful for anyone to disturb the King's officer who comes to execute the King's process; for if a man might stand out in such manner a man would never have execution, but there it appears (as has been said) that there ought to be request made before the sheriff breaks [into] the house:

(d) the sheriffs were officers of great authority in whom the law reposed great trust and confidence, and are to be of sufficiency to answer for all wrongs which should be done; and they had custodia comitatem, and, therefore, it should not be presumed that they would abuse the house of anyone by colour of doing their office in execution of the King's writs against the duty of their office and their oath also.

But it was resolved that it is not lawful for the sheriff (on request made and denial) at the suit of a common person to break [into] the defendant's house, scilicet, to execute any process at the suit of any subject, for thence would follow great inconvenience that men as well in the night as in the day should have their houses (which are their castles) broken into, by colour whereof great damage and mischief might ensue; for by colour thereof, on any feigned suit, the house of any man at any time might be broken into when the defendant might be arrested elsewhere, and so men would not be in safety or quiet in their own houses. And although the sheriff is an officer of great authority and trust, yet it appears by experience that the King's writs are served by bailiffs, persons of little or no value; and it is not to be presumed that all the substance a man has in his house, nor that a man would lose his liberty which is so inestimable, if he has sufficient to satisfy his debt.

And all the said books which prove that, when the process concerns the King, the sheriff may break [into] the house, imply that at the suit of the party the house may not be broken into], otherwise the addition (at the suit of the King) would be frivolous. And with this resolution agrees the book in YB 13 Edw 4, fo 9, pl 4. The

express difference there taken between the case of felony, which (as has been said) concerns the commonwealth, and the suit of any subject, which is for the particular interest of the party, as there it is said in YB 18 Edw 4, fo 4, pl 19, by LITTLETON and all his companions that it is resolved that the sheriff cannot break [into] the defendant's house by force of a fieri facias but he is a trespasser by the breaking, and yet the execution which he then does in the house is good. It was said that the book of 18 Edw 2 was but a short note and not any case judicially adjudged and it does not appear at whose suit the case is intended, but it is an observation or collection (as it seems) of the reporter. And if it be intended of a quo minus or other action in which the King is party or is to have benefit, the book is good law.

(v) That the house of anyone is not a castle or privilege but for himself, and shall not extend to protect any person who flies to his house or the goods of any other which are brought and conveyed into his house to prevent a lawful execution and to escape the ordinary process of law; for the privilege of his house extends only to him and his family, and to his own proper goods, or to those which are lawfully and without fraud and covin there, and, therefore, in such cases after denial on request made, the sheriff may break [into] the house. That is proved by the First Statute of Westminster, c 17 [repealed], by which it is declared that the sheriff may break [into] a house or castle to make replevin when the goods of another which he has distrained are by him conveyed to his house or castle to prevent the owner to have a replevin of his goods; which Act is but an affirmance of the common law in such points. But it appears there that, before the sheriff in such case breaks [into] the house, he ought to demand the goods to be delivered to him, for the words of the statute are: "After that the cattle shall be solemnly demanded by the sheriff's, etc."

(vi) That admitting that the sheriff after denial might have broken into the house, as the plaintiff's counsel pretend he might, then it follows that he has not done his duty, for it does not appear that be made any request to open the door of the house. Also the defendant, as this case is, has done that which he might well do by the law, scilicet, to shut the door of his own house.

Lastly, the general allegation praemissorum non ignarus was not sufficient in this case where the notice of the premises is so material; but in this case it ought to have been certainly and directly alleged; for without notice of the process of law and of the coming of the sheriff with the jury to execute it, the shutting of the door of his own house was lawful. Judgment was given against the plaintiff.

DISPOSITION:
Judgment for defendant.

Terry v. Ohio (No. 67)

Syllabus	Opinion [Warren]	Concurrence [Harlan]	Concurrence [White]	Dissent [Fortas]
HTML version PDF version	HTML version PDF version	HTML version PDF version	HTML version PDF version	HTML version PDF version

WARREN, C.J., Opinion of the Court

SUPREME COURT OF THE UNITED STATES

Read 10/11

392 U.S. 1

Terry v. Ohio

CERTIORARI TO THE SUPREME COURT OF OHIO

No. 67 Argued: December 12, 1967 --- Decided: June 10, 1968

MR. CHIEF JUSTICE WARREN delivered the opinion of the Court.

This case presents serious questions concerning the role of the Fourth Amendment in the confrontation on the street between the citizen and the policeman investigating suspicious circumstances.

Petitioner Terry was convicted of carrying a concealed weapon and sentenced to the statutorily prescribed term of one to three years in the penitentiary. [n1] Following [p5] the denial of a pretrial motion to suppress, the prosecution introduced in evidence two revolvers and a number of bullets seized from Terry and a codefendant, Richard Chilton, [n2] by Cleveland Police Detective Martin McFadden. At the hearing on the motion to suppress this evidence, Officer McFadden testified that, while he was patrolling in plain clothes in downtown Cleveland at approximately 2:30 in the afternoon of October 31, 1963, his attention was attracted by two men, Chilton and Terry, standing on the corner of Huron Road and Euclid Avenue. He had never seen the two men before, and he was unable to say precisely what first drew his eye to them. However, he testified that he had been a policeman for 39 years and a detective for 35, and that he had been assigned to patrol this vicinity of downtown Cleveland for shoplifters and pickpockets for 30 years. He explained that he had developed routine habits of observation over the years, and that he would "stand and watch people or walk and watch people at many intervals of the day." He added: "Now, in this case, when I looked over, they didn't look right to me at the time."

Vague

His interest aroused, Officer McFadden took up a post of observation in the entrance to a store 300 to 400 feet [p6] away from the two men. "I get more purpose to watch them when I seen their movements," he testified. He saw one of the men leave the other one and walk southwest on Huron Road, past some stores. The man paused for a moment and looked in a store window, then walked on a short distance, turned around and walked back toward the corner, pausing once again to look in the same store window. He rejoined his companion at the corner, and the two conferred briefly. Then the second man went through the same series of motions, strolling down Huron Road, looking in the same window, walking on a short distance, turning back, peering in the store window again, and returning to confer with the first man at the corner. The two men repeated this

ritual alternately between five and six times apiece -- in all, roughly a dozen trips. At one point, while the two were standing together on the corner, a third man approached them and engaged them briefly in conversation. This man then left the two others and walked west on Euclid Avenue. Chilton and Terry resumed their measured pacing, peering, and conferring. After this had gone on for 10 to 12 minutes, the two men walked off together, heading west on Euclid Avenue, following the path taken earlier by the third man.

By this time, Officer McFadden had become thoroughly suspicious. He testified that, after observing their elaborately casual and oft-repeated reconnaissance of the store window on Huron Road, he suspected the two men of "casing a job, a stick-up," and that he considered it his duty as a police officer to investigate further. He added that he feared "they may have a gun." Thus, Officer McFadden followed Chilton and Terry and saw them stop in front of Zucker's store to talk to the same man who had conferred with them earlier on the street corner. Deciding that the situation was ripe for direct action, Officer McFadden approached the three men, identified [p7] himself as a police officer and asked for their names. At this point, his knowledge was confined to what he had observed. He was not acquainted with any of the three men by name or by sight, and he had received no information concerning them from any other source. When the men "mumbled something" in response to his inquiries, Officer McFadden grabbed petitioner Terry, spun him around so that they were facing the other two, with Terry between McFadden and the others, and patted down the outside of his clothing. In the left breast pocket of Terry's overcoat, Officer McFadden felt a pistol. He reached inside the overcoat pocket, but was unable to remove the gun. At this point, keeping Terry between himself and the others, the officer ordered all three men to enter Zucker's store. As they went in, he removed Terry's overcoat completely, removed a .38 caliber revolver from the pocket and ordered all three men to face the wall with their hands raised. Officer McFadden proceeded to pat down the outer clothing of Chilton and the third man, Katz. He discovered another revolver in the outer pocket of Chilton's overcoat, but no weapons were found on Katz. The officer testified that he only patted the men down to see whether they had weapons, and that he did not put his hands beneath the outer garments of either Terry or Chilton until he felt their guns. So far as appears from the record, he never placed his hands beneath Katz' outer garments. Officer McFadden seized Chilton's gun, asked the proprietor of the store to call a police wagon, and took all three men to the station, where Chilton and Terry were formally charged with carrying concealed weapons.

On the motion to suppress the guns, the prosecution took the position that they had been seized following a search incident to a lawful arrest. The trial court rejected this theory, stating that it "would be stretching the facts beyond reasonable comprehension" to find that Officer [p8] McFadden had had probable cause to arrest the men before he patted them down for weapons. However, the court denied the defendants' motion on the ground that Officer McFadden, on the basis of his experience,

> had reasonable cause to believe . . . that the defendants were conducting themselves suspiciously, and some interrogation should be made of their action.

Purely for his own protection, the court held, the officer had the right to pat down the outer clothing of these men, who he had reasonable cause to believe might be armed. The court distinguished between an investigatory "stop" and an arrest, and between a "frisk" of the outer clothing for weapons and a full-blown search for evidence of crime. The frisk, it held, was essential to the proper performance of the officer's investigatory duties, for, without it, "the answer to the police officer may be a bullet, and a loaded pistol discovered during the frisk is admissible."

After the court denied their motion to suppress, Chilton and Terry waived jury trial and pleaded not guilty. The court adjudged them guilty, and the Court of Appeals for the Eighth Judicial District, Cuyahoga County, affirmed. *State v. Terry*, 5 Ohio App.2d 122, 214 N.E.2d 114 (1966). The Supreme Court of Ohio dismissed their appeal on the ground that no "substantial constitutional question"

arrested for what
Mm

? this is ok right?

was involved. We granted certiorari, 387 U.S. 929 (1967), to determine whether the admission of the revolvers in evidence violated petitioner's rights under the Fourth Amendment, made applicable to the States by the Fourteenth. *Mapp v. Ohio*, 367 U.S. 643 (1961). We affirm the conviction.

I

The Fourth Amendment provides that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated. . . ." This inestimable right of [p9] personal security belongs as much to the citizen on the streets of our cities as to the homeowner closeted in his study to dispose of his secret affairs. For as this Court has always recognized,

> No right is held more sacred, or is more carefully guarded, by the common law than the right of every individual to the possession and control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law.

Union Pac. R. Co. v. Botsford, 141 U.S. 250, 251 (1891). We have recently held that "the Fourth Amendment protects people, not places," *Katz v. United States*, 389 U.S. 347, 351 (1967), and wherever an individual may harbor a reasonable "expectation of privacy," *id.* at 361 (MR. JUSTICE HARLAN, concurring), he is entitled to be free from unreasonable governmental intrusion. Of course, the specific content and incidents of this right must be shaped by the context in which it is asserted. For "what the Constitution forbids is not all searches and seizures, but unreasonable searches and seizures." *Elkins v. United States*, 364 U.S. 206, 222 (1960). Unquestionably petitioner was entitled to the protection of the Fourth Amendment as he walked down the street in Cleveland. *Beck v. Ohio*, 379 U.S. 89 (1964); *Rios v. United States*, 364 U.S. 253 (1960); *Henry v. United States*, 361 U.S. 98 (1959); *United States v. Di Re*, 332 U.S. 581 (1948); *Carroll v. United States*, 267 U.S. 132 (1925). The question is whether, in all the circumstances of this on-the-street encounter, his right to personal security was violated by an unreasonable search and seizure.

We would be less than candid if we did not acknowledge that this question thrusts to the fore difficult and troublesome issues regarding a sensitive area of police activity -- issues which have never before been squarely [p10] presented to this Court. Reflective of the tensions involved are the practical and constitutional arguments pressed with great vigor on both sides of the public debate over the power of the police to "stop and frisk" -- as it is sometimes euphemistically termed -- suspicious persons.

On the one hand, it is frequently argued that, in dealing with the rapidly unfolding and often dangerous situations on city streets, the police are in need of an escalating set of flexible responses, graduated in relation to the amount of information they possess. For this purpose, it is urged that distinctions should be made between a "stop" and an "arrest" (or a "seizure" of a person), and between a "frisk" and a "search." [n3] Thus, it is argued, the police should be allowed to "stop" a person and detain him briefly for questioning upon suspicion that he may be connected with criminal activity. Upon suspicion that the person may be armed, the police should have the power to "frisk" him for weapons. If the "stop" and the "frisk" give rise to probable cause to believe that the suspect has committed a crime, then the police should be empowered to make a formal "arrest," and a full incident "search" of the person. This scheme is justified in part upon the notion that a "stop" and a "frisk" amount to a mere "minor inconvenience and petty indignity," [n4] which can properly be imposed upon the [p11] citizen in the interest of effective law enforcement on the basis of a police officer's suspicion. [n5]

On the other side, the argument is made that the authority of the police must be strictly circumscribed by the law of arrest and search as it has developed to date in the traditional jurisprudence of the Fourth Amendment. [n6] It is contended with some force that there is not -- and cannot be -- a variety of police activity which does not depend solely upon the voluntary cooperation of the citizen, and

hwd to set express rules

yet which stops short of an arrest based upon probable cause to make such an arrest. The heart of the Fourth Amendment, the argument runs, is a severe requirement of specific justification for any intrusion upon protected personal security, coupled with a highly developed system of judicial controls to enforce upon the agents of the State the commands of the Constitution. Acquiescence by the courts in the compulsion inherent [p12] in the field interrogation practices at issue here, it is urged, would constitute an abdication of judicial control over, and indeed an encouragement of, substantial interference with liberty and personal security by police officers whose judgment is necessarily colored by their primary involvement in "the often competitive enterprise of ferreting out crime." *Johnson v. United States*, 333 U.S. 10, 14 (1948). This, it is argued, can only serve to exacerbate police-community tensions in the crowded centers of our Nation's cities. [n7]

In this context, we approach the issues in this case mindful of the limitations of the judicial function in controlling the myriad daily situations in which policemen and citizens confront each other on the street. The State has characterized the issue here as

> the right of a police officer . . . to make an on-the-street stop, interrogate and pat down for weapons (known in street vernacular as "stop and frisk"). [n8]

But this is only partly accurate. For the issue is not the abstract propriety of the police conduct, but the admissibility against petitioner of the evidence uncovered by the search and seizure. Ever since its inception, the rule excluding evidence seized in violation of the Fourth Amendment has been recognized as a principal mode of discouraging lawless police conduct. *See Weeks v. United States*, 232 U.S. 383, 391-393 (1914). Thus, its major thrust is a deterrent one, *see Linkletter v. Walker*, 381 U.S. 618, 629-635 (1965), and experience has taught that it is the only effective deterrent to police misconduct in the criminal context, and that, without it, the constitutional guarantee against unreasonable searches and seizures would be a mere "form of words." *Mapp v. Ohio*, 367 U.S. 643, 655 (1961). The rule also serves another vital function -- "the imperative of judicial integrity." *Elkins* [p13] *v. United States*, 364 U.S. 206, 222 (1960). Courts which sit under our Constitution cannot and will not be made party to lawless invasions of the constitutional rights of citizens by permitting unhindered governmental use of the fruits of such invasions. Thus, in our system, evidentiary rulings provide the context in which the judicial process of inclusion and exclusion approves some conduct as comporting with constitutional guarantees and disapproves other actions by state agents. A ruling admitting evidence in a criminal trial, we recognize, has the necessary effect of legitimizing the conduct which produced the evidence, while an application of the exclusionary rule withholds the constitutional imprimatur.

The exclusionary rule has its limitations, however, as a tool of judicial control. It cannot properly be invoked to exclude the products of legitimate police investigative techniques on the ground that much conduct which is closely similar involves unwarranted intrusions upon constitutional protections. Moreover, in some contexts, the rule is ineffective as a deterrent. Street encounters between citizens and police officers are incredibly rich in diversity. They range from wholly friendly exchanges of pleasantries or mutually useful information to hostile confrontations of armed men involving arrests, or injuries, or loss of life. Moreover, hostile confrontations are not all of a piece. Some of them begin in a friendly enough manner, only to take a different turn upon the injection of some unexpected element into the conversation. Encounters are initiated by the police for a wide variety of purposes, some of which are wholly unrelated to a desire to prosecute for crime. [n9] Doubtless some [p14] police "field interrogation" conduct violates the Fourth Amendment. But a stern refusal by this Court to condone such activity does not necessarily render it responsive to the exclusionary rule. Regardless of how effective the rule may be where obtaining convictions is an important objective of the police, [n10] it is powerless to deter invasions of constitutionally guaranteed rights where the police either have no interest in prosecuting or are willing to forgo successful prosecution in the interest of

serving some other goal.

Proper adjudication of cases in which the exclusionary rule is invoked demands a constant awareness of these limitations. The wholesale harassment by certain elements of the police community, of which minority groups, particularly Negroes, frequently complain, [n11] will not be [p15] stopped by the exclusion of any evidence from any criminal trial. Yet a rigid and unthinking application of the exclusionary rule, in futile protest against practices which it can never be used effectively to control, may exact a high toll in human injury and frustration of efforts to prevent crime. No judicial opinion can comprehend the protean variety of the street encounter, and we can only judge the facts of the case before us. Nothing we say today is to be taken as indicating approval of police conduct outside the legitimate investigative sphere. Under our decision, courts still retain their traditional responsibility to guard against police conduct which is overbearing or harassing, or which trenches upon personal security without the objective evidentiary justification which the Constitution requires. When such conduct is identified, it must be condemned by the judiciary, and its fruits must be excluded from evidence in criminal trials. And, of course, our approval of legitimate and restrained investigative conduct undertaken on the basis of ample factual justification should in no way discourage the employment of other remedies than the exclusionary rule to curtail abuses for which that sanction may prove inappropriate.

Having thus roughly sketched the perimeters of the constitutional debate over the limits on police investigative conduct in general and the background against which this case presents itself, we turn our attention to the quite narrow question posed by the facts before us: whether it is always unreasonable for a policeman to seize a person and subject him to a limited search for weapons unless there is probable cause for an arrest. [p16] Given the narrowness of this question, we have no occasion to canvass in detail the constitutional limitations upon the scope of a policeman's power when he confronts a citizen without probable cause to arrest him.

II

Our first task is to establish at what point in this encounter the Fourth Amendment becomes relevant. That is, we must decide whether and when Officer McFadden "seized" Terry, and whether and when he conducted a "search." There is some suggestion in the use of such terms as "stop" and "frisk" that such police conduct is outside the purview of the Fourth Amendment because neither action rises to the level of a "search" or "seizure" within the meaning of the Constitution. [n12] We emphatically reject this notion. It is quite plain that the Fourth Amendment governs "seizures" of the person which do not eventuate in a trip to the stationhouse and prosecution for crime -- "arrests" in traditional terminology. It must be recognized that, whenever a police officer accosts an individual and restrains his freedom to walk away, he has "seized" that person. And it is nothing less than sheer torture of the English language to suggest that a careful exploration of the outer surfaces of a person's clothing all over his or her body in an attempt to find weapons is not a "search." Moreover, it is simply fantastic to urge that such a procedure [p17] performed in public by a policeman while the citizen stands helpless, perhaps facing a wall with his hands raised, is a "petty indignity." [n13] It is a serious intrusion upon the sanctity of the person, which may inflict great indignity and arouse strong resentment, and it is not to be undertaken lightly. [n14]

TBA

The danger in the logic which proceeds upon distinctions between a "stop" and an "arrest," or "seizure" of the person, and between a "frisk" and a "search," is twofold. It seeks to isolate from constitutional scrutiny the initial stages of the contact between the policeman and the citizen. And, by suggesting a rigid all-or-nothing model of justification and regulation under the Amendment, it obscures the utility of limitations upon the scope, as well as the initiation, of police action as a means of constitutional regulation. [n15] This Court has held, in [p18] the past that a search which is reasonable at its inception may violate the Fourth Amendment by virtue of its intolerable intensity and scope. *Kremen v. United*

States, 353 U.S. 346 (1957); *Go-Bart Importing Co. v.* [p19] *United States*, 282 U.S. 344, 356-358 (1931); *see United States v. Di Re*, 332 U.S. 581, 586-587 (1948). The scope of the search must be "strictly tied to and justified by" the circumstances which rendered its initiation permissible. *Warden v. Hayden*, 387 U.S. 294, 310 (1967) (MR. JUSTICE FORTAS, concurring); *see, e.g., Preston v. United States*, 376 U.S. 364, 367-368 (1964); *Agnello v. United States*, 269 U.S. 20, 30-31 (1925).

The distinctions of classical "stop-and-frisk" theory thus serve to divert attention from the central inquiry under the Fourth Amendment -- the reasonableness in all the circumstances of the particular governmental invasion of a citizen's personal security. "Search" and "seizure" are not talismans. We therefore reject the notions that the Fourth Amendment does not come into play at all as a limitation upon police conduct if the officers stop short of something called a "technical arrest" or a "full-blown search."

In this case, there can be no question, then, that Officer McFadden "seized" petitioner and subjected him to a "search" when he took hold of him and patted down the outer surfaces of his clothing. We must decide whether, at that point, it was reasonable for Officer McFadden to have interfered with petitioner's personal security as he did. [n16] And, in determining whether the seizure and search were "unreasonable," our inquiry [p20] is a dual one -- whether the officer's action was justified at its inception, and whether it was reasonably related in scope to the circumstances which justified the interference in the first place.

expose each fragment of the issue

III

If this case involved police conduct subject to the Warrant Clause of the Fourth Amendment, we would have to ascertain whether "probable cause" existed to justify the search and seizure which took place. However, that is not the case. We do not retreat from our holdings that the police must, whenever practicable, obtain advance judicial approval of searches and seizures through the warrant procedure, *see, e.g., Katz v. United States*, 389 U.S. 347 (1967); *Beck v. Ohio*, 379 U.S. 89, 96 (1964); *Chapman v. United States*, 365 U.S. 610 (1961), or that, in most instances, failure to comply with the warrant requirement can only be excused by exigent circumstances, *see, e.g., Warden v. Hayden*, 387 U.S. 294 (1967) (hot pursuit); *cf. Preston v. United States*, 376 U.S. 364, 367-368 (1964). But we deal here with an entire rubric of police conduct -- necessarily swift action predicated upon the on-the-spot observations of the officer on the beat -- which historically has not been, and, as a practical matter, could not be, subjected to the warrant procedure. Instead, the conduct involved in this case must be tested by the Fourth Amendment's general proscription against unreasonable searches and seizures. [n17]

Nonetheless, the notions which underlie both the warrant procedure and the requirement of probable cause remain fully relevant in this context. In order to assess the reasonableness of Officer McFadden's conduct as a general proposition, it is necessary "first to focus upon [p21] the governmental interest which allegedly justifies official intrusion upon the constitutionally protected interests of the private citizen," for there is

> no ready test for determining reasonableness other than by balancing the need to search [or seize] against the invasion which the search [or seizure] entails.

Camara v. Municipal Court, 387 U.S. 523, 534-535, 536-537 (1967). And, in justifying the particular intrusion, the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion. [n18] The scheme of the Fourth Amendment becomes meaningful only when it is assured that, at some point, the conduct of those charged with enforcing the laws can be subjected to the more detached, neutral scrutiny of a judge who must evaluate the reasonableness of a particular search or seizure in light of the particular circumstances. [n19] And, in making that assessment, it is imperative that the facts be judged against an

objective standard: would the facts [p22] available to the officer at the moment of the seizure or the search "warrant a man of reasonable caution in the belief" that the action taken was appropriate? *Cf. Carroll v. United States*, 267 U.S. 132 (1925); *Beck v. Ohio*, 379 U.S. 89, 96-97 (1964).[n20] Anything less would invite intrusions upon constitutionally guaranteed rights based on nothing more substantial than inarticulate hunches, a result this Court has consistently refused to sanction. *See, e.g., Beck v. Ohio, supra; Rios v. United States*, 364 U.S. 253 (1960); *Henry v. United States*, 361 U.S. 98 (1959). And simple

> "good faith on the part of the arresting officer is not enough." . . . If subjective good faith alone were the test, the protections of the Fourth Amendment would evaporate, and the people would be "secure in their persons, houses, papers, and effects," only in the discretion of the police.

Beck v. Ohio, supra, at 97.

Applying these principles to this case, we consider first the nature and extent of the governmental interests involved. One general interest is, of course, that of effective crime prevention and detection; it is this interest which underlies the recognition that a police officer may, in appropriate circumstances and in an appropriate manner, approach a person for purposes of investigating possibly criminal behavior even though there is no probable cause to make an arrest. It was this legitimate investigative function Officer McFadden was discharging when he decided to approach petitioner and his companions. He had observed Terry, Chilton, and Katz go through a series of acts, each of them perhaps innocent in itself, but which, taken together, warranted further investigation. There is nothing unusual in two men standing together on a street corner, perhaps waiting for someone. Nor is there anything suspicious about people [p23] in such circumstances strolling up and down the street, singly or in pairs. Store windows, moreover, are made to be looked in. But the story is quite different where, as here, two men hover about a street corner for an extended period of time, at the end of which it becomes apparent that they are not waiting for anyone or anything; where these men pace alternately along an identical route, pausing to stare in the same store window roughly 24 times; where each completion of this route is followed immediately by a conference between the two men on the corner; where they are joined in one of these conferences by a third man who leaves swiftly, and where the two men finally follow the third and rejoin him a couple of blocks away. It would have been poor police work indeed for an officer of 30 years' experience in the detection of thievery from stores in this same neighborhood to have failed to investigate this behavior further.

The crux of this case, however, is not the propriety of Officer McFadden's taking steps to investigate petitioner's suspicious behavior, but, rather, whether there was justification for McFadden's invasion of Terry's personal security by searching him for weapons in the course of that investigation. We are now concerned with more than the governmental interest in investigating crime; in addition, there is the more immediate interest of the police officer in taking steps to assure himself that the person with whom he is dealing is not armed with a weapon that could unexpectedly and fatally be used against him. Certainly it would be unreasonable to require that police officers take unnecessary risks in the performance of their duties. American criminals have a long tradition of armed violence, and every year in this country many law enforcement officers are killed in the line of duty, and thousands more are wounded. [p24] Virtually all of these deaths and a substantial portion of the injuries are inflicted with guns and knives.[n21]

Can any police search someone when taking

In view of these facts, we cannot blind ourselves to the need for law enforcement officers to protect themselves and other prospective victims of violence in situations where they may lack probable cause for an arrest. When an officer is justified in believing that the individual whose suspicious behavior he is investigating at close range is armed and presently dangerous to the officer or to others, it would appear to be clearly unreasonable to deny the officer the power to take necessary measures to determine whether the person is, in fact, carrying a weapon and to neutralize the threat of physical harm.

We must still consider, however, the nature and quality of the intrusion on individual rights which must be accepted if police officers are to be conceded the right to search for weapons in situations where probable cause to arrest for crime is lacking. Even a limited search of the outer clothing for weapons constitutes a severe, [p25] though brief, intrusion upon cherished personal security, and it must surely be an annoying, frightening, and perhaps humiliating experience. Petitioner contends that such an intrusion is permissible only incident to a lawful arrest, either for a crime involving the possession of weapons or for a crime the commission of which led the officer to investigate in the first place. However, this argument must be closely examined.

) esp in NY
-can stop for any reason

Petitioner does not argue that a police officer should refrain from making any investigation of suspicious circumstances until such time as he has probable cause to make an arrest; nor does he deny that police officers, in properly discharging their investigative function, may find themselves confronting persons who might well be armed and dangerous. Moreover, he does not say that an officer is always unjustified in searching a suspect to discover weapons. Rather, he says it is unreasonable for the policeman to take that step until such time as the situation evolves to a point where there is probable cause to make an arrest. When that point has been reached, petitioner would concede the officer's right to conduct a search of the suspect for weapons, fruits or instrumentalities of the crime, or "mere" evidence, incident to the arrest.

There are two weaknesses in this line of reasoning, however. First, it fails to take account of traditional limitations upon the scope of searches, and thus recognizes no distinction in purpose, character, and extent between a search incident to an arrest and a limited search for weapons. The former, although justified in part by the acknowledged necessity to protect the arresting officer from assault with a concealed weapon, *Preston v. United States*, 376 U.S. 364, 367 (1964), is also justified on other grounds, *ibid.*, and can therefore involve a relatively extensive exploration of the person. A search for weapons in the absence of probable cause to [p26] arrest, however, must, like any other search, be strictly circumscribed by the exigencies which justify its initiation. *Warden v. Hayden*, 387 U.S. 294, 310 (1967) (MR. JUSTICE FORTAS, concurring). Thus, it must be limited to that which is necessary for the discovery of weapons which might be used to harm the officer or others nearby, and may realistically be characterized as something less than a "full" search, even though it remains a serious intrusion.

A second, and related, objection to petitioner's argument is that it assumes that the law of arrest has already worked out the balance between the particular interests involved here -- the neutralization of danger to the policeman in the investigative circumstance and the sanctity of the individual. But this is not so. An arrest is a wholly different kind of intrusion upon individual freedom from a limited search for weapons, and the interests each is designed to serve are likewise quite different. An arrest is the initial stage of a criminal prosecution. It is intended to vindicate society's interest in having its laws obeyed, and it is inevitably accompanied by future interference with the individual's freedom of movement, whether or not trial or conviction ultimately follows.[n22] The protective search for weapons, on the other hand, constitutes a brief, though far from inconsiderable, intrusion upon the sanctity of the person. It does not follow that, because an officer may lawfully arrest a person only when he is apprised of facts sufficient to warrant a belief that the person has committed or is committing a crime, the officer is equally unjustified, absent that kind of evidence, in making any intrusions short of an arrest. Moreover, a perfectly reasonable apprehension of danger may arise long before the officer is possessed of adequate information to justify taking a person into custody for [p27] the purpose of prosecuting him for a crime. Petitioner's reliance on cases which have worked out standards of reasonableness with regard to "seizures" constituting arrests and searches incident thereto is thus misplaced. It assumes that the interests sought to be vindicated and the invasions of personal security may be equated in the two cases, and thereby ignores a vital aspect of the analysis of the reasonableness of particular types of conduct under the Fourth Amendment. *See Camara v. Municipal Court, supra.*

of evidence of crime. *See Preston v. United States*, 376 U.S. 364, 367 (1964). The sole justification of the search in the present situation is the protection of the police officer and others nearby, and it must therefore be confined in scope to an intrusion reasonably designed to discover guns, knives, clubs, or other hidden instruments for the assault of the police officer.

The scope of the search in this case presents no serious problem in light of these standards. Officer McFadden patted down the outer clothing of petitioner and his two companions. He did not place his hands in their pockets or under the outer surface of their garments until he had [p30] felt weapons, and then he merely reached for and removed the guns. He never did invade Katz' person beyond the outer surfaces of his clothes, since he discovered nothing in his pat-down which might have been a weapon. Officer McFadden confined his search strictly to what was minimally necessary to learn whether the men were armed and to disarm them once he discovered the weapons. He did not conduct a general exploratory search for whatever evidence of criminal activity he might find.

V

We conclude that the revolver seized from Terry was properly admitted in evidence against him. At the time he seized petitioner and searched him for weapons, Officer McFadden had reasonable grounds to believe that petitioner was armed and dangerous, and it was necessary for the protection of himself and others to take swift measures to discover the true facts and neutralize the threat of harm if it materialized. The policeman carefully restricted his search to what was appropriate to the discovery of the particular items which he sought. Each case of this sort will, of course, have to be decided on its own facts. We merely hold today that, where a police officer observes unusual conduct which leads him reasonably to conclude in light of his experience that criminal activity may be afoot and that the persons with whom he is dealing may be armed and presently dangerous, where, in the course of investigating this behavior, he identifies himself as a policeman and makes reasonable inquiries, and where nothing in the initial stages of the encounter serves to dispel his reasonable fear for his own or others' safety, he is entitled for the protection of himself and others in the area to conduct a carefully limited search of the outer clothing of such persons in an attempt to discover weapons which might be used to assault him. [p31] Such a search is a reasonable search under the Fourth Amendment, and any weapons seized may properly be introduced in evidence against the person from whom they were taken.

Affirmed.

MR. JUSTICE BLACK concurs in the judgment and the opinion except where the opinion quotes from and relies upon this Court's opinion in *Katz v. United States* and the concurring opinion in *Warden v. Hayden*.

1. Ohio Rev.Code § 2923.01 (1953) provides in part that "[n]o person shall carry a pistol, bowie knife, dirk, or other dangerous weapon concealed on or about his person." An exception is made for properly authorized law enforcement officers.

2. Terry and Chilton were arrested, indicted, tried, and convicted together. They were represented by the same attorney, and they made a joint motion to suppress the guns. After the motion was denied, evidence was taken in the case against Chilton. This evidence consisted of the testimony of the arresting officer and of Chilton. It was then stipulated that this testimony would be applied to the case against Terry, and no further evidence was introduced in that case. The trial judge considered the two cases together, rendered the decisions at the same time, and sentenced the two men at the same time. They prosecuted their state court appeals together through the same attorney, and they petitioned this Court for certiorari together. Following the grant of the writ upon this joint petition, Chilton died. Thus, only Terry's conviction is here for review.

3. Both the trial court and the Ohio Court of Appeals in this case relied upon such a distinction. State v. Terry, 5 Ohio App.2d 122, 125-130, 214 N.E.2d 114, 117-120 (1966). See also, e.g., People v. Rivera, 14 N.Y.2d 441, 201 N.E.2d 32,

Our evaluation of the proper balance that has to be struck in this type of case leads us to conclude that there must be a narrowly drawn authority to permit a reasonable search for weapons for the protection of the police officer, where he has reason to believe that he is dealing with an armed and dangerous individual, regardless of whether he has probable cause to arrest the individual for a crime. The officer need not be absolutely certain that the individual is armed; the issue is whether a reasonably prudent man, in the circumstances, would be warranted in the belief that his safety or that of others was in danger. *Cf. Beck v. Ohio*, 379 U.S. 89, 91 (1964); *Brinegar v. United States*, 338 U.S. 160, 174-176 (1949); *Stacey v. Emery*, 97 U.S. 642, 645 (1878). [n23] And in determining whether the officer acted reasonably in such circumstances, due weight must be given not to his inchoate and unparticularized suspicion or "hunch," but to the specific reasonable inferences which he is entitled to draw from the facts in light of his experience. *Cf. Brinegar v. United States supra.*

IV

We must now examine the conduct of Officer McFadden in this case to determine whether his search and seizure of petitioner were reasonable, both at their inception [p28] and as conducted. He had observed Terry, together with Chilton and another man, acting in a manner he took to be preface to a "stick-up." We think, on the facts and circumstances Officer McFadden detailed before the trial judge, a reasonably prudent man would have been warranted in believing petitioner was armed, and thus presented a threat to the officer's safety while he was investigating his suspicious behavior. The actions of Terry and Chilton were consistent with McFadden's hypothesis that these men were contemplating a daylight robbery -- which, it is reasonable to assume, would be likely to involve the use of weapons -- and nothing in their conduct from the time he first noticed them until the time he confronted them and identified himself as a police officer gave him sufficient reason to negate that hypothesis. Although the trio had departed the original scene, there was nothing to indicate abandonment of an intent to commit a robbery at some point. Thus, when Officer McFadden approached the three men gathered before the display window at Zucker's store, he had observed enough to make it quite reasonable to fear that they were armed, and nothing in their response to his hailing them, identifying himself as a police officer, and asking their names served to dispel that reasonable belief. We cannot say his decision at that point to seize Terry and pat his clothing for weapons was the product of a volatile or inventive imagination, or was undertaken simply as an act of harassment; the record evidences the tempered act of a policeman who, in the course of an investigation, had to make a quick decision as to how to protect himself and others from possible danger, and took limited steps to do so.

good explanation for this

The manner in which the seizure and search were conducted is, of course, as vital a part of the inquiry as whether they were warranted at all. The Fourth Amendment proceeds as much by limitations upon the [p29] scope of governmental action as by imposing preconditions upon its initiation. *Compare Katz v. United States*, 389 U.S. 347, 354-356 (1967). The entire deterrent purpose of the rule excluding evidence seized in violation of the Fourth Amendment rests on the assumption that "limitations upon the fruit to be gathered tend to limit the quest itself." *United States v. Poller*, 43 F.2d 911, 914 (C.A.2d Cir.1930); *see, e.g., Linkletter v. Walker*, 381 U.S. 618, 629-635 (1965); *Mapp v. Ohio*, 367 U.S. 643 (1961); *Elkins v. United States*, 364 U.S. 206, 216-221 (1960). Thus, evidence may not be introduced if it was discovered by means of a seizure and search which were not reasonably related in scope to the justification for their initiation. *Warden v. Hayden*, 387 U.S. 294, 310 (1967) (MR. JUSTICE FORTAS, concurring).

We need not develop at length in this case, however, the limitations which the Fourth Amendment places upon a protective seizure and search for weapons. These limitations will have to be developed in the concrete factual circumstances of individual cases. *See Sibron v. New York, post*, p. 40, decided today. Suffice it to note that such a search, unlike a search without a warrant incident to a lawful arrest, is not justified by any need to prevent the disappearance or destruction

252 N.Y.S.2d 458 (1964), cert. denied, 379 U.S. 978 (1965); Aspen, Arrest and Arrest Alternatives: Recent Trends, 1966 U.Ill.L.F. 241, 249-254; Warner, The Uniform Arrest Act, 28 Va.L.Rev. 315 (1942); Note, Stop and Frisk in California, 18 Hastings L.J. 623, 629-632 (1967).

4. People v. Rivera, supra, n. 3, at 447, 201 N.E.2d at 36, 252 N.Y.S.2d at 464.

5. The theory is well laid out in the Rivera opinion:

> [T]he evidence needed to make the inquiry is not of the same degree of conclusiveness as that required for an arrest. The stopping of the individual to inquire is not an arrest and the ground upon which the police may make the inquiry may be less incriminating than the ground for an arrest for a crime known to have been committed. . . .
>
> * * * *
>
> And as the right to stop and inquire is to be justified for a cause less conclusive than that which would sustain an arrest, so the right to frisk may be justified as an incident to inquiry upon grounds of elemental safety and precaution which might not initially sustain a search. Ultimately, the validity of the frisk narrows down to whether there is or is not a right by the police to touch the person questioned. The sense of exterior touch here involved is not very far different from the sense of sight or hearing -- senses upon which police customarily act.

People v. Rivera, 14 N.Y.2d 441, 445, 447, 201 N.E.2d 32, 34, 35, 252 N.Y.S.2d 458, 461, 463 (1964), *cert. denied*, 379 U.S. 978 (1965).

6. See, e.g., Foote, The Fourth Amendment: Obstacle or Necessity in the Law of Arrest?, 51 J.Crim.L.C. & P.S. 402 (1960).

7. See n. 11, infra.

8. Brief for Respondent 2.

9. See L. Tiffany, D. McIntyre D. Rotenberg, Detection of Crime: Stopping and Questioning, Search and Seizure, Encouragement and Entrapment 186 (1967). This sort of police conduct may, for example, be designed simply to help an intoxicated person find his way home, with no intention of arresting him unless he becomes obstreperous. Or the police may be seeking to mediate a domestic quarrel which threatens to erupt into violence. They may accost a woman in an area known for prostitution as part of a harassment campaign designed to drive prostitutes away without the considerable difficulty involved in prosecuting them. Or they may be conducting a dragnet search of all teenagers in a particular section of the city for weapons because they have heard rumors of an impending gang fight.

10. See Tiffany, McIntyre & Rotenberg, supra, n. 9, at 100-101; Comment, 47 Nw.U.L.Rev. 493, 497-499 (1952).

11. The President's Commission on Law Enforcement and Administration of Justice found that, "[i]n many communities, field interrogations are a major source of friction between the police and minority groups." President's Commission on Law Enforcement and Administration of Justice, Task Force Report: The Police 183 (1967). It was reported that the friction caused by "[m]isuse of field interrogations" increases

> as more police departments adopt "aggressive patrol," in which officers are encouraged routinely to stop and question persons on the street who are unknown to them, who are suspicious, or whose purpose for being abroad is not readily evident.

Id. at 184. While the frequency with which "frisking" forms a part of field interrogation practice varies tremendously with the locale, the objective of the interrogation, and the particular officer, *see* Tiffany, McIntyre & Rotenberg, *supra*, n. 9, at 47-48, it cannot help but be a severely exacerbating factor in

police-community tensions. This is particularly true in situations where the "stop and frisk" of youths or minority group members is

> motivated by the officers' perceived need to maintain the power image of the beat officer, an aim sometimes accomplished by humiliating anyone who attempts to undermine police control of the streets.

Ibid.

12. In this case, for example, the Ohio Court of Appeals stated that

> we must be careful to distinguish that the "frisk" authorized herein includes only a "frisk" for a dangerous weapon. It by no means authorizes a search for contraband, evidentiary material, or anything else in the absence of reasonable grounds to arrest. Such a search is controlled by the requirements of the Fourth Amendment, and probable cause is essential.

State v. Terry, 5 Ohio App.2d 122, 130, 214 N.E.2d 114, 120 (1966). *See also, e.g., Ellis v. United States*, 105 U.S.App.D.C. 86, 88, 264 F.2d 372, 374 (1959); Comment, 65 Col.L.Rev. 848, 860, and n. 81 (1965).

13. Consider the following apt description:

> [T]he officer must feel with sensitive fingers every portion of the prisoner's body. A thorough search must be made of the prisoner's arms and armpits, waistline and back, the groin and area about the testicles, and entire surface of the legs down to the feet.

Priar & Martin, Searching and Disarming Criminals, 45 J.Crim.L.C. & P.S. 481 (1954).

14. See n. 11, supra, and accompanying text.

We have noted that the abusive practices which play a major, though by no means exclusive, role in creating this friction are not susceptible of control by means of the exclusionary rule, and cannot properly dictate our decision with respect to the powers of the police in genuine investigative and preventive situations. However, the degree of community resentment aroused by particular practices is clearly relevant to an assessment of the quality of the intrusion upon reasonable expectations of personal security caused by those practices.

15. These dangers are illustrated in part by the course of adjudication in the Court of Appeals of New York. Although its first decision in this area, People v. Rivera, 14 N.Y.2d 441, 201 N.E.2d 32, 252 N.Y.S.2d 458 (1964), cert. denied, 379 U.S. 978 (1965), rested squarely on the notion that a "frisk" was not a "search," see nn. 3-5, supra, it was compelled to recognize, in People v. Taggart, 20 N.Y.2d 335, 342, 229 N.E.2d 581, 586, 283 N.Y.S.2d 1, 8 (1967), that what it had actually authorized in Rivera and subsequent decisions, see, e.g., People v. Pugach, 15 N.Y.2d 65, 204 N.E.2d 176, 255 N.Y.S.2d 833 (1964), cert. denied, 380 U.S. 936 (1965), was a "search" upon less than probable cause. However, in acknowledging that no valid distinction could be maintained on the basis of its cases, the Court of Appeals continued to distinguish between the two in theory. It still defined "search" as it had in Rivera -- as an essentially unlimited examination of the person for any and all seizable items -- and merely noted that the cases had upheld police intrusions which went far beyond the original limited conception of a "frisk." Thus, principally because it failed to consider limitations upon the scope of searches in individual cases as a potential mode of regulation, the Court of Appeals in three short years arrived at the position that the Constitution must, in the name of necessity, be held to permit unrestrained rummaging about a person and his effects upon mere suspicion. It did apparently limit its holding to "cases involving serious personal injury or grave irreparable property damage," thus excluding those involving "the enforcement of sumptuary laws, such as gambling, and laws of limited public consequence, such as narcotics violations, prostitution, larcenies of the ordinary kind, and the like." People v. Taggart, supra, at 340, 214 N.E.2d at 584, 283 N.Y.S.2d at 6.

In our view, the sounder course is to recognize that the Fourth Amendment governs all intrusions by agents of the public upon personal security, and to make the scope of the particular intrusion, in light of all the exigencies of the case, a central element in the analysis of reasonableness. *Cf. Brinegar v. United States*, 338 U.S. 160, 183 (1949) (Mr. Justice Jackson, dissenting). *Compare Camara v. Municipal Court*, 387 U.S. 523, 537 (1967). This seems preferable to an approach which attributes too much significance to an overly technical definition of "search," and which turns in part upon a judge-made hierarchy of legislative enactments in the criminal sphere. Focusing the inquiry squarely on the dangers and demands of the particular situation also seems more likely to produce rules which are intelligible to the police and the public alike than requiring the officer in the heat of an unfolding encounter on the street to make a judgment as to which laws are "of limited public consequence."

16. We thus decide nothing today concerning the constitutional propriety of an investigative "seizure" upon less than probable cause for purposes of "detention" and/or interrogation. Obviously, not all personal intercourse between policemen and citizens involves "seizures" of persons. Only when the officer, by means of physical force or show of authority, has in some way restrained the liberty of a citizen may we conclude that a "seizure" has occurred. We cannot tell with any certainty upon this record whether any such "seizure" took place here prior to Officer McFadden's initiation of physical contact for purposes of searching Terry for weapons, and we thus may assume that, up to that point, no intrusion upon constitutionally protected rights had occurred.

17. See generally Leagre, The Fourth Amendment and the Law of Arrest, 54 J.Crim.L.C. & P.S. 393, 396 403 (1963).

18. This demand for specificity in the information upon which police action is predicated is the central teaching of this Court's Fourth Amendment jurisprudence. See Beck v. Ohio, 379 U.S. 89, 96-97 (1964); Ker v. California, 374 U.S. 23, 34-37 (1963); Wong Sun v. United States, 371 U.S. 471, 479-484 (1963); Rios v. United States, 364 U.S. 253, 261-262 (1960); Henry v. United States, 361 U.S. 98, 100-102 (1959); Draper v. United States, 358 U.S. 307, 312-314 (1959); Brinegar v. United States, 338 U.S. 160, 175-178 (1949); Johnson v. United States, 333 U.S. 10, 15-17 (1948); United States v. Di Re, 332 U.S. 581, 593-595 (1948); Husty v. United States, 282 U.S. 694, 700-701 (1931); Dumbra v. United States, 268 U.S. 435, 441 (1925); Carroll v. United States, 267 U.S. 132, 159-162 (1925); Stacey v. Emery, 97 U.S. 642,645 (1878).

19. See, e.g., Katz v. United States, 389 U.S. 347, 354-357 (1967); Berger v. New York, 388 U.S. 41, 54-60 (1967); Johnson v. United States, 333 U.S. 10, 13-15 (1948); cf. Wong Sun v. United States, 371 U.S. 471, 479-480 (1963). See also Aguilar v. Texas, 378 U.S. 108, 110-115 (1964).

20. See also cases cited in n. 18, supra.

21. Fifty-seven law enforcement officers were killed in the line of duty in this country in 1966, bringing the total to 335 for the seven-year period beginning with 1960. Also in 1966, there were 23,851 assaults on police officers, 9,113 of which resulted in injuries to the policemen. Fifty-five of the 57 officers killed in 1966 died from gunshot wounds, 41 of them inflicted by handguns easily secreted about the person. The remaining two murders were perpetrated by knives. See Federal Bureau of Investigation, Uniform Crime Reports for the United States -- 1966, at 45-48, 152 and Table 51.

The easy availability of firearms to potential criminals in this country is well known, and has provoked much debate. *See, e.g.*, President's Commission on Law Enforcement and Administration of Justice, The Challenge of Crime in a Free Society 239-243 (1967). Whatever the merits of gun control proposals, this fact is relevant to an assessment of the need for some form of self-protective search power.

22. See generally W. LaFave, Arrest -- The Decision to Take a Suspect into Custody 1-13 (1965).

[23] See also cases cited in n. 18, supra.

Supreme Court

ABOUT SEARCH SUBSCRIBE LIIBULLETIN PREVIEWS

Olmstead v. United States () 100 U.S. 1
19 F. (2d) 842, 848, 850, affirmed.

Syllabus	Opinion [Taft]	Separate [Holmes]	Dissent [Brandeis]	Dissent [Butler]	Dissent [Stone]
HTML version PDF version	HTML version PDF version	HTML version PDF version	HTML version PDF version	HTML version PDF version	HTML version PDF version

Syllabus

Read 10/11

SUPREME COURT OF THE UNITED STATES

277 U.S. 438

Olmstead v. United States

CERTIORARI TO THE CIRCUIT COURT OF APPEALS FOR THE NINTH CIRCUIT

Argued: February 20, 21, 1928 — Decided: June 4, 1928

1. Use in evidence in a criminal trial in a federal court of an incriminating telephone conversation voluntarily conducted by the accused and secretly overheard from a tapped wire by a government officer does not compel the accused to be a witness against himself in violation of the Fifth Amendment. P. 462.

2. Evidence of a conspiracy to violate the Prohibition Act was obtained by government officers by secretly tapping the lines of a telephone company connected with the chief office and some of the residences of the conspirators, and thus clandestinely overhearing and recording their telephonic conversations concerning the conspiracy and in aid of its execution. The tapping connections were made in the basement of a large office building and on public streets, and no trespass was committed upon any property of the defendants. *Held*, that the obtaining of the evidence and its use at the trial did not violate the Fourth Amendment. Pp. 457-466.

warrant?

lots of cases on where this applies

3. The principle of liberal construction applied to the Amendment to effect its purpose in the interest of liberty will not justify enlarging it beyond the possible practical meaning of "persons, houses, papers, and effects," or so applying "searches and seizures" as to forbid hearing or sight. P. 465.

4. The policy of protecting the secrecy of telephone messages by making them, when intercepted, inadmissible as evidence in federal criminal trials may be adopted by Congress through legislation, but it is not for the courts to adopt it by attributing an enlarged and unusual meaning to the Fourth Amendment. P. 465.

5. A provision in an order granting certiorari limiting the review to a single specific question does not deprive the Court of jurisdiction to decide other questions presented by the record. P. 466.

6. The common law of evidence having prevailed in the State of Washington since a time antedating her transformation from a [p439] Territory to a State, those rule apply in the trials of criminal cases in the federal courts sitting in that State. P. 466.

7. Under the common law, the admissibility of evidence is not affected by the fact of its having been obtained illegally. P. 467.

8. The rule excluding from the federal Courts evidence of crime procured by government officers by methods forbidden by the Fourth and Fifth Amendments is an exception to the common law rule. *Id.*

9. Without the sanction of an Act of Congress, federal courts have no discretion to exclude evidence, the admission of which is not unconstitutional, because it was unethically procured. P. 468.

10. The statute of Washington, adopted in 1909, making the interception of telephone messages a misdemeanor cannot affect the rules of evidence applicable in federal courts in criminal cases. *Id.*

CERTIORARI, 276 U.S. 609, to judgments of the Circuit Court of Appeals affirming convictions of conspiracy to violate the Prohibition Act. *See* 5 F.2d 712; 7 F.2d 756, 760. The order granting certiorari confined the hearing to the question whether the use in evidence of private telephone conversations, intercepted by means of wiretapping, violated the Fourth and Fifth Amendments. [p455]

Supreme Court

ABOUT SEARCH SUBSCRIBE LIIBULLETIN PREVIEWS

Katz v. United States (No. 35)

Syllabus	Opinion [Stewart]	Concurrence [Douglas]	Concurrence [Harlan]	Concurrence [White]	Dissent [Black]
HTML version PDF version	HTML version PDF version	HTML version PDF version	HTML version PDF version	HTML version PDF version	HTML version PDF version

STEWART, J., Opinion of the Court

SUPREME COURT OF THE UNITED STATES

Read 10/4 in class

389 U.S. 347

Katz v. United States

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

No. 35 Argued: October 17, 1967 --- Decided: December 18, 1967

MR. JUSTICE STEWART delivered the opinion of the Court.

The petitioner was convicted in the District Court for the Southern District of California under an eight-count indictment charging him with transmitting wagering information by telephone from Los Angeles to Miami and Boston, in violation of a federal statute.[n1] At trial, the Government was permitted, over the petitioner's objection, to introduce evidence of the petitioner's end of telephone conversations, overheard by FBI agents who had attached an electronic listening and recording device to the outside of the public telephone booth from which he had placed his calls. In affirming his conviction, the Court of Appeals rejected the contention that the recordings had been obtained in violation of the Fourth Amendment, [p349] because "[t]here was no physical entrance into the area occupied by [the petitioner]."[n2] We granted certiorari in order to consider the constitutional questions thus presented.[n3]

technical arguments but should it cover?

The petitioner has phrased those questions as follows:

> A. Whether a public telephone booth is a constitutionally protected area so that evidence obtained by attaching an electronic listening recording device to the top of such a booth is obtained in violation of the right to privacy of the user of the booth. [p350]
>
> B. Whether physical penetration of a constitutionally protected area is necessary before a search and seizure can be said to be violative of the Fourth Amendment to the United States Constitution.

We decline to adopt this formulation of the issues. In the first place, the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase "constitutionally protected area." Secondly, the Fourth Amendment cannot be translated into a general constitutional "right to privacy." That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all.[n4] Other provisions of the Constitution protect personal

privacy from other forms of governmental invasion.[n5] But the protection of a person's *general* right to privacy -- his right to be let alone by other people[n6] -- is, like the [p351] protection of his property and of his very life, left largely to the law of the individual States.[n7]

Because of the misleading way the issues have been formulated, the parties have attached great significance to the characterization of the telephone booth from which the petitioner placed his calls. The petitioner has strenuously argued that the booth was a "constitutionally protected area." The Government has maintained with equal vigor that it was not.[n8] But this effort to decide whether or not a given "area," viewed in the abstract, is "constitutionally protected" deflects attention from the problem presented by this case.[n9] For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. *See Lewis v. United States*, 385 U.S. 206, 210; *United States v. Lee*, 274 U.S. 559, 563. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected. [p352] *See Rios v. United States*, 364 U.S. 253; *Ex parte Jackson*, 96 U.S. 727, 733.

The Government stresses the fact that the telephone booth from which the petitioner made his calls was constructed partly of glass, so that he was as visible after he entered it as he would have been if he had remained outside. But what he sought to exclude when he entered the booth was not the intruding eye -- it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen. No less than an individual in a business office,[n10] in a friend's apartment,[n11] or in a taxicab,[n12] a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.

The Government contends, however, that the activities of its agents in this case should not be tested by Fourth Amendment requirements, for the surveillance technique they employed involved no physical penetration of the telephone booth from which the petitioner placed his calls. It is true that the absence of such penetration was at one time thought to foreclose further Fourth Amendment inquiry, *Olmstead v. United States*, 277 U.S. 438, 457, 464, 466; *Goldman v. United States*, 316 U.S. 129, 134-136, for that Amendment was thought to limit only searches and seizures of tangible [p353] property.[n13] But "[t]he premise that property interests control the right of the Government to search and seize has been discredited." *Warden v. Hayden*, 387 U.S. 294, 304. Thus, although a closely divided Court supposed in *Olmstead* that surveillance without any trespass and without the seizure of any material object fell outside the ambit of the Constitution, we have since departed from the narrow view on which that decision rested. Indeed, we have expressly held that the Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements, overheard without any "technical trespass under . . . local property law." *Silverman v. United States*, 365 U.S. 505, 511. Once this much is acknowledged, and once it is recognized that the Fourth Amendment protects people -- and not simply "areas" -- against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.

We conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the "trespass" doctrine there enunciated can no longer be regarded as controlling. The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth, and thus constituted a "search and seizure" within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance. [p354]

The question remaining for decision, then, is whether the search and seizure conducted in this case complied with constitutional standards. In that regard, the Government's position is that its agents acted in an entirely defensible manner: they did not begin their electronic surveillance until investigation of the petitioner's activities had established a strong probability that he was using the telephone in question to transmit gambling information to persons in other States, in violation of federal law. Moreover, the surveillance was limited, both in scope and in duration, to the specific purpose of establishing the contents of the petitioner's unlawful telephonic communications. The agents confined their surveillance to the brief periods during which he used the telephone booth, [n14] and they took great care to overhear only the conversations of the petitioner himself. [n15]

Accepting this account of the Government's actions as accurate, it is clear that this surveillance was so narrowly circumscribed that a duly authorized magistrate, properly notified of the need for such investigation, specifically informed of the basis on which it was to proceed, and clearly apprised of the precise intrusion it would entail, could constitutionally have authorized, with appropriate safeguards, the very limited search and seizure that the Government asserts, in fact, took place. Only last Term we sustained the validity of [p355] such an authorization, holding that, under sufficiently "precise and discriminate circumstances," a federal court may empower government agents to employ a concealed electronic device "for the narrow and particularized purpose of ascertaining the truth of the . . . allegations" of a "detailed factual affidavit alleging the commission of a specific criminal offense." *Osborn v. United States*, 385 U.S. 323, 329-330. Discussing that holding, the Court in *Berger v. New York*, 388 U.S. 41, said that "the order authorizing the use of the electronic device" in *Osborn* "afforded similar protections to those . . . of conventional warrants authorizing the seizure of tangible evidence." Through those protections, "no greater invasion of privacy was permitted than was necessary under the circumstances." *Id.* at 57. [n16] Here, too, a similar [p356] judicial order could have accommodated "the legitimate needs of law enforcement" [n17] by authorizing the carefully limited use of electronic surveillance.

The Government urges that, because its agents relied upon the decisions in *Olmstead* and *Goldman*, and because they did no more here than they might properly have done with prior judicial sanction, we should retroactively validate their conduct. That we cannot do. It is apparent that the agents in this case acted with restraint. Yet the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer. They were not required, before commencing the search, to present their estimate of probable cause for detached scrutiny by a neutral magistrate. They were not compelled, during the conduct of the search itself, to observe precise limits established in advance by a specific court order. Nor were they directed, after the search had been completed, to notify the authorizing magistrate in detail of all that had been seized. In the absence of such safeguards, this Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive [p357] means consistent with that end. Searches conducted without warrants have been held unlawful "notwithstanding facts unquestionably showing probable cause," *Agnello v. United States*, 269 U.S. 20, 33, for the Constitution requires "that the deliberate, impartial judgment of a judicial officer . . . be interposed between the citizen and the police. . . ." *Wong Sun v. United States*, 371 U.S. 471, 481-482. "Over and again, this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes," *United States v. Jeffers*, 342 U.S. 48, 51, and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment [n18] -- subject only to a few specifically established and well delineated exceptions. [n19]

It is difficult to imagine how any of those exceptions could ever apply to the sort of search and seizure involved in this case. Even electronic surveillance substantially contemporaneous with an individual's arrest could hardly be deemed

an "incident" of that arrest. [n20] [p358] Nor could the use of electronic surveillance without prior authorization be justified on grounds of "hot pursuit." [n21] And, of course, the very nature of electronic surveillance precludes its use pursuant to the suspect's consent. [n22]

The Government does not question these basic principles. Rather, it urges the creation of a new exception to cover this case. [n23] It argues that surveillance of a telephone booth should be exempted from the usual requirement of advance authorization by a magistrate upon a showing of probable cause. We cannot agree. Omission of such authorization

> bypasses the safeguards provided by an objective predetermination of probable cause, and substitutes instead the far less reliable procedure of an after-the-event justification for the . . . search, too likely to be subtly influenced by the familiar shortcomings of hindsight judgment.

Beck v. Ohio, 379 U.S. 89, 96. And bypassing a neutral predetermination of the scope of a search leaves individuals secure from Fourth Amendment [p359] violations "only in the discretion of the police." *Id.* at 97.

These considerations do not vanish when the search in question is transferred from the setting of a home, an office, or a hotel room to that of a telephone booth. Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures. The government agents here ignored "the procedure of antecedent justification . . . that is central to the Fourth Amendment," [n24] a procedure that we hold to be a constitutional precondition of the kind of electronic surveillance involved in this case. Because the surveillance here failed to meet that condition, and because it led to the petitioner's conviction, the judgment must be reversed.

It is so ordered.

MR. JUSTICE MARSHALL took no part in the consideration or decision of this case.

1. 18 U.S.C. § 1084. That statute provides in pertinent part:

> (a) Whoever being engaged in the business of betting or wagering knowingly uses a wire communication facility for the transmission in interstate or foreign commerce of bets or wagers or information assisting in the placing of bets or wagers on any sporting event or contest, or for the transmission of a wire communication which entitles the recipient to receive money or credit as a result of bets or wagers, or for information assisting in the placing of bets or wagers, shall be fined not more than $10,000 or imprisoned not more than two years, or both.
>
> (b) Nothing in this section shall be construed to prevent the transmission in interstate or foreign commerce of information for use in news reporting of sporting events or contests, or for the transmission of information assisting in the placing of bets or wagers on a sporting event or contest from a State where betting on that sporting event or contest is legal into a State in which such betting is legal.

2. 369 F.2d 130, 134

3. 386 U.S. 954. The petition for certiorari also challenged the validity of a warrant authorizing the search of the petitioner's premises. In light of our disposition of this case, we do not reach that issue.

We find no merit in the petitioner's further suggestion that his indictment must be dismissed. After his conviction was affirmed by the Court of Appeals, he testified before a federal grand jury concerning the charges involved here. Because he was compelled to testify pursuant to a grant of immunity, 48 Stat. 1096, as amended, 47 U.S.C. § 409(*l*), it is clear that the fruit of his testimony cannot be used against him in any future trial. But the petitioner asks for more. He contends that. his conviction must be vacated and the charges against him dismissed lest he

be "subjected to [a] penalty . . . on account of [a] . . . matter . . . concerning which he [was] compelled . . . to testify. . . ." 47 U.S.C. § 409(*l*). *Frank v. United States*, 347 F.2d 486. We disagree. In relevant part, § 409(*l*) substantially repeats the language of the Compulsory Testimony Act of 1893, 27 Stat. 443, 49 U.S.C. § 46 which was Congress' response to this Court's statement that an immunity statute can supplant the Fifth Amendment privilege against self-incrimination only if it affords adequate protection from future prosecution or conviction. *Counselman v. Hitchcock*, 142 U.S. 547, 585-586. The statutory provision here involved was designed to provide such protection, *see Brown v. United States*, 359 U.S. 41, 45-46, not to confer immunity from punishment pursuant to a *prior* prosecution and adjudication of guilt. *Cf. Regina v. United States*, 364 U.S. 507, 513-514.

4.

> The average man would very likely not have his feelings soothed any more by having his property seized openly than by having it seized privately and by stealth. . . . And a person can be just as much, if not more, irritated, annoyed and injured by an unceremonious public arrest by a policeman as he is by a seizure in the privacy of his office or home.

Griswold v. Connecticut, 381 U.S. 479, 509 (dissenting opinion of MR. JUSTICE BLACK).

5. The First Amendment, for example, imposes limitations upon governmental abridgment of "freedom to associate and privacy in one's associations." NAACP v. Alabama, 357 U.S. 449, 462. The Third Amendment's prohibition against the unconsented peacetime quartering of soldiers protects another aspect of privacy from governmental intrusion. To some extent, the Fifth Amendment too "reflects the Constitution's concern for . . . '. . . the right of each individual "to a private enclave where he may lead a private life."" Tehan v. Shott, 382 U.S. 406, 416. Virtually every governmental action interferes with personal privacy to some degree. The question in each case is whether that interference violates a command of the United States Constitution.

6. See Warren & Brandeis, The Right to Privacy, 4 Harv.L.Rev.193 (1890).

7. See, e.g., Time, Inc. v. Hill, 385 U.S. 374. Cf. Breard v. Alexandria, 341 U.S. 622; Kovacs v. Cooper, 336 U.S. 77.

8. In support of their respective claims, the parties have compiled competing lists of "protected areas" for our consideration. It appears to be common ground that a private home is such an area, Weeks v. United States, 232 U.S. 383, but that an open field is not. Hester v. United States, 265 U.S. 57. Defending the inclusion of a telephone booth in his list the petitioner cites United States v. Stone, 232 F.Supp. 396, and United States v. Madison, 32 L.W. 2243 (D.C. Ct.Gen.Sess.). Urging that the telephone booth should be excluded, the Government finds support in United States v. Borgese, 235 F.Supp. 286.

9. It is true that this Court has occasionally described its conclusions in terms of "constitutionally protected areas," see, e.g., Silverman v. United States, 365 U.S. 505, 510, 512; Lopez v. United States, 373 U.S. 427, 438-439; Berger v. New York, 388 U.S. 41, 57, 59, but we have never suggested that this concept can serve as a talismanic solution to every Fourth Amendment problem.

10. Silverthorne Lumber Co. v. United States, 251 U.S. 385.

11. Jones v. United States, 362 U.S. 257.

12. Rios v United States, 364 U.S. 253.

13. See Olmstead v. United States, 277 U.S. 438, 464-466. We do not deal in this case with the law of detention or arrest under the Fourth Amendment.

14. Based upon their previous visual observations of the petitioner, the agents correctly predicted that he would use the telephone booth for several minutes at

approximately the same time each morning. The petitioner was subjected to electronic surveillance only during this predetermined period. Six recordings, averaging some three minutes each, were obtained and admitted in evidence. They preserved the petitioners end of conversations concerning the placing of bets and the receipt of wagering information.

15. On the single occasion when the statements of another person were inadvertently intercepted, the agents refrained from listening to them.

16. Although the protections afforded the petitioner in Osborn were "similar . . . to those . . . of conventional warrants," they were not identical. A conventional warrant ordinarily serves to notify the suspect of an intended search. But if Osborn had been told in advance that federal officers intended to record his conversations, the point of making such recordings would obviously have been lost; the evidence in question could not have been obtained. In omitting any requirement of advance notice, the federal court that authorized electronic surveillance in Osborn simply recognized, as has this Court, that officers need not announce their purpose before conducting an otherwise authorized search if such an announcement would provoke the escape of the suspect or the destruction of critical evidence. See Ker v. California, 374 U.S. 23, 37-41.

Although some have thought that this "exception to the notice requirement where exigent circumstances are present," *id.* at 39, should be deemed inapplicable where police enter a home before its occupants are aware that officers are present, *id.* at 55-58 (opinion of MR. JUSTICE BRENNAN), the reasons for such a limitation have no bearing here. However true it may be that "[i]nnocent citizens should not suffer the shock, fright or embarrassment attendant upon an unannounced police intrusion," *id.* at 57, and that "the requirement of awareness . . . serves to minimize the hazards of the officers' dangerous calling," *id.* at 57-58, these considerations are not relevant to the problems presented by judicially authorized electronic surveillance.

Nor do the Federal Rules of Criminal Procedure impose an inflexible requirement of prior notice.Rule 41(d) does require federal officers to serve upon the person searched a copy of the warrant and a receipt describing the material obtained, but it does not invariably require that this be done before the search takes place. *Nordelli v. United States*, 24 F.2d 665, 666-667.

Thus, the fact that the petitioner in *Osborn* was unaware that his words were being electronically transcribed did not prevent this Court from sustaining his conviction, and did not prevent the Court in *Berger* from reaching the conclusion that the use of the recording device sanctioned in *Osborn* was entirely lawful. 388 U.S. 41, 57.

17. Lopez v. United States, 373 U.S. 427, 464 (dissenting opinion of MR. JUSTICE BRENNAN).

18. See, e.g., Jones v. United States, 357 U.S. 493, 497-499; Rios v. United States, 364 U.S. 253, 261; Chapman v. United States, 365 U.S. 610, 613-615; Stoner v. California, 376 U.S. 483, 486-487.

19. See, e.g., Carroll v. United States, 267 U.S. 132, 153, 156; McDonald v. United States, 335 U.S. 451, 454-456; Brinegar v. United States, 338 U.S. 160, 174-177; Cooper v. California, 386 U.S. 58; Warden v. Hayden, 387 U.S. 294, 298-300.

20. In Agnello v. United States, 269 U.S. 20, 30, the Court stated:

> The right without a search warrant contemporaneously to search persons lawfully arrested while committing crime and to search the place where the arrest is made in order to find and seize things connected with the crime as its fruits or as the means by which it was committed, as well as weapons and other things to effect an escape from custody, is not to be doubted.

Whatever one's view of "the longstanding practice of searching for other proofs of

guilt within the control of the accused found upon arrest," *United States v. Rabinowitz*, 339 U.S. 56, 61; *cf. id.* at 71-79 (dissenting opinion of Mr. Justice Frankfurter), the concept of an "incidental" search cannot readily be extended to include surreptitious surveillance of an individual either immediately before, or immediately after, his arrest.

21. Although

> [t]he Fourth Amendment does not require police officers to delay in the course of an investigation if to do so would gravely endanger their lives or the lives of others,

Warden v. Hayden, 387 U.S. 294, 298-299, there seems little likelihood that electronic surveillance would be a realistic possibility in a situation so fraught with urgency.

22. A search to which an individual consents meets Fourth Amendment requirements, Zap v. United States, 328 U.S. 624, but, of course, "the usefulness of electronic surveillance depends on lack of notice to the suspect." Lopez v. United States, 373 U.S. 427, 463 (dissenting opinion of MR. JUSTICE BRENNAN).

23. Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case.

24. See Osborn v. United States, 385 U.S. 323, 330.

99TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
99-647

ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

JUNE 19, 1986.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. KASTENMEIER, from the Committee on the Judiciary, submitted the following

REPORT

[To accompany H.R. 4952]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 4952) to amend title 18, United States Code, with respect to the interception of certain communications, other forms of surveillance, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment is as follows:

Strike out all after the enacting clause and insert in lieu thereof the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Electronic Communications Privacy Act of 1986".

TITLE I—INTERCEPTION OF COMMUNICATIONS AND RELATED MATTERS

SEC. 101. FEDERAL PENALTIES FOR THE INTERCEPTION OF COMMUNICATIONS.

(a) DEFINITIONS.—(1) Section 2510(1) of title 18, United States Code, is amended—

(A) by striking out "any communication" and inserting "any aural transfer" in lieu thereof;

(B) by inserting "(including the use of such connection in a switching station)" after "reception";

(C) by striking out "as a common carrier" and

(D) by inserting before the semicolon at the end the following: "or communications affecting interstate or foreign commerce, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit".

(2) Section 2510(2) of title 18, United States Code, is amended by inserting before the semicolon at the end the following: ", but such term does not include any electronic communication".

(3) Section 2510(4) of title 18, United States Code, is amended—

(A) by inserting "or other" after "aural"; and

61-068 O

(B) by inserting ", electronic," after "wire".

(4) Section 2510(8) of title 18, United States Code, is amended by striking out "identity of the parties to such communication or the existence,".

(5) Section 2510 of title 18, United States Code, is amended—

(A) by striking out "and" at the end of paragraph (10);

(B) by striking out the period at the end of paragraph (11) and inserting a semicolon in lieu thereof; and

(C) by adding at the end the following:

"(12) 'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

"(A) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;

"(B) any wire or oral communication;

"(C) any communication made through a tone-only paging device; or

"(D) any communication from a tracking device (as defined in section 3117 of this title);

"(13) 'user' means any person or entity who—

"(A) uses an electronic communication service; and

"(B) is duly authorized by the provider of such service to engage in such use;

"(14) 'electronic communications system' means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

"(15) 'electronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications;

"(16) 'readily accessible to the general public' means, with respect to a radio communication, that such communication is not—

"(A) scrambled or encrypted;

"(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

"(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

"(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

"(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

"(17) 'electronic storage' means—

"(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

"(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; and

"(18) 'aural transfer' means a transfer containing the human voice at any point between and including the point of origin and the point of reception.".

(b) EXCEPTIONS WITH RESPECT TO ELECTRONIC COMMUNICATIONS.—

(1) Section 2511(2)(d) of title 18, United States Code, is amended by striking out "or for the purpose of committing any other injurious act".

(2) Section 2511(2)(f) of title 18, United States Code, is amended—

(A) by inserting "or chapter 121" after "this chapter"; and

(B) by striking out "by" the second place it appears and inserting in lieu thereof ", or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing".

(3) Section 2511(2) of title 18, United States Code, is amended by adding at the end the following:

"(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—

"(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

"(ii) to intercept any radio communication which is transmitted—

"(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

"(II) by any governmental, law enforcement, civil defense, or public safety communications system, including police and fire, readily accessible to the general public;

"(III) by a station operating on a frequency assigned to the amateur, citizens band, or general mobile radio services; or

"(IV) by any marine or aeronautical communications system;

"(iii) to engage in any conduct which—

"(I) is prohibited by section 633 of the Communications Act of 1934; or

"(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

"(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station, to the extent necessary to identify the source of such interference; or

"(v) for other users of the same frequency to intercept any radio communication made through a common carrier system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled encrypted.

"(h) It shall not be unlawful under this chapter—

"(i) to use a pen register (as that term is defined for the purposes of chapter 206 (relating to pen registers) of this title);

"(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service; or

"(iii) to use a device that captures the incoming electronic or other impulses which identify the numbers of an instrument from which a wire communication was transmitted.".

(c) TECHNICAL AND CONFORMING AMENDMENTS.—(1) Chapter 119 of title 18, United States Code, is amended—

(A) in each of sections 2510(5), 2510(8), 2510(9)(b), 2510(11), and 2511 through 2519 (except sections 2516(1) and 2518(10)), by striking out "wire or oral" each place it appears (including in any section heading) and inserting "wire, oral, or electronic" in lieu thereof; and

(B) in section 2511(2)(b), by inserting "or electronic" after "wire".

(2) The heading of chapter 119 of title 18, United States Code, is amended by inserting "**and electronic communications**" after "**wire**".

(3) The item relating to chapter 119 in the table of chapters at the beginning of part I of title 18 of the United States Code is amended by inserting "and electronic communications" after "Wire".

(4) Section 2510(5)(a) of title 18, United States Code, is amended by striking out "communications common carrier" and inserting "provider of wire or electronic communication service" in lieu thereof.

(5) Section 2511(2)(a)(i) of title 18, United States Code, is amended—

(A) by striking out "any communication common carrier" and inserting "a provider of wire or electronic communication service" in lieu thereof;

(B) by striking out "of the carrier of such communication" and inserting "of the provider of that service" in lieu thereof; and

(C) by striking out ": *Provided*, That said communication common carriers" and inserting ", except that a provider of wire communication service to the public" in lieu thereof.

(6) Section 2511(2)(a)(ii) of title 18, United States Code, is amended—

(A) by striking out "communication common carriers" and inserting "providers of wire or electronic communication service" in lieu thereof;

(B) by striking out "communication common carrier" each place it appears and inserting "provider of wire or electronic communication service" in lieu thereof; and

(C) by striking out "if the common carrier" and inserting "if such provider" in lieu thereof.

(7) Section 2512(2)(a) of title 18, United States Code, is amended—

(A) by striking out "a communications common carrier" the first place it appears and inserting "a provider of wire or electronic communication service" in lieu thereof; and

(B) by striking out "a communications common carrier" the second place it appears and inserting "such a provider" in lieu thereof; and

(C) by striking out "communications common carrier's business" and inserting "business of providing that wire or electronic communication service" in lieu thereof.

(8) Section 2518(4) of title 18, United States Code, is amended by striking out "communication common carrier" and inserting "provider of electronic communication service" in lieu thereof.

(d) PENALTIES MODIFICATION.—(1) Section 2511(1) of title 18, United States Code, is amended by striking out "shall be" and all that follows through "or both" and inserting in lieu thereof "shall be punished as provided in subsection (4)".

(2) Section 2511 of title 18, United States Code, is amended by adding after the material added by section 102 the following:

"(4)(a) Except as provided in paragraph (b) of this subsection, whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

"(b) If the offense is a first offense under paragraph (a) of this subsection and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication, then—

"(i) if the communication is not the radio portion of a cellular telephone communication, the offender shall be fined under this title or imprisoned not more than one year, or both; and

"(ii) if the communication is the radio portion of a cellular telephone communication, the offender shall be fined not more than $500 or imprisoned not more than six months, or both.

"(c) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted to a broadcasting station for purposes of retransmission to the general public is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.".

(e) EXCLUSIVITY OF REMEDIES WITH RESPECT TO ELECTRONIC COMMUNICATIONS.—Section 2518(10) of title 18, United States Code, is amended by adding at the end the following:

"(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.".

SEC. 102. REQUIREMENTS FOR CERTAIN DISCLOSURES.

Section 2511 of title 18, United States Code, is amended by adding at the end the following:

"(3)(A) Except as provided in subparagraph (B) of this paragraph, a person or entity providing an electronic communication service to the public shall not willfully divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

"(B) A person or entity providing electronic communication service to the public may divulge the contents of any such communication—

"(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

"(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

"(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

"(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.".

SEC. 103. RECOVERY OF CIVIL DAMAGES.

Section 2520 of title 18, United States Code, is amended to read as follows:

"§ 2520. Recovery of civil damages authorized

"(a) IN GENERAL.—Any person whose wire, oral, or electronic communication is intercepted, disclosed, or willfully used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

"(b) RELIEF.—In an action under this section, appropriate relief includes—

"(1) such preliminary and other equitable or declaratory relief as may be appropriate;

"(2) damages under subsection (c) and punitive damages in appropriate cases; and

"(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

"(c) COMPUTATION OF DAMAGES.—The court may assess as damages in an action under this section whichever is the greater of—

"(1) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

"(2) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

"(d) DEFENSE.—A good faith reliance on—

"(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

"(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

"(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter or any other provision of law.

"(e) LIMITATION.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.".

SEC. 104. CERTAIN APPROVALS BY JUSTICE DEPARTMENT OFFICIALS.

Section 2516(1) of title 18 of the United States Code is amended by striking out "or any Assistant Attorney General" and inserting in lieu thereof "any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division".

SEC. 105. ADDITION OF OFFENSES TO CRIMES FOR WHICH INTERCEPTION IS AUTHORIZED.

(a) WIRE AND ORAL INTERCEPTIONS.—Section 2516(1) of title 18 of the United States Code is amended—

(1) in paragraph (c)—

(A) by inserting "section 751 (relating to escape)," after "wagering information),";

(B) by striking out "2314" and inserting "2312, 2313, 2314," in lieu thereof;

(C) by inserting "the second section 2320 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities)," after "stolen property),";

(D) by inserting "section 1952A (relating to use of interstate commerce facilities in the commission of murder for hire), section 1952B (relating to violent crimes in aid of racketeering activity)," after "1952 (interstate and foreign travel or transportation in aid of racketeering enterprises),"; and

(E) by inserting ", section 115 (relating to threatening or retaliating against a Federal official), the section in chapter 65 relating to destruction of an energy facility, and section 1341 (relating to mail fraud)," after "section 1963 (violations with respect to racketeer influenced and corrupt organizations)";

(2) by striking out "or" at the end of paragraph (g);

(3) by inserting after paragraph (g) the following:

"(h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain intercepting devices) of this title;

"(i) the location of any fugitive from justice from an offense described in this section; or"; and

(4) by redesignating paragraph (h) as paragraph (j).

(b) INTERCEPTION OF ELECTRONIC COMMUNICATIONS.—Section 2516 of title 18 of the United States Code is amended by adding at the end the following:

"(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.".

SEC. 106. APPLICATIONS, ORDERS, AND IMPLEMENTATION OF ORDERS.

(a) PLACE OF AUTHORIZED INTERCEPTION.—Section 2518(3) of title 18 of the United States Code is amended by inserting "(and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction)" after "within the territorial jurisdiction of the court in which the judge is sitting".

(b) REIMBURSEMENT FOR ASSISTANCE.—Section 2518(4) of title 18 of the United States Code is amended by striking out "at the prevailing rates" and inserting in lieu thereof "for reasonable expenses incurred in providing such facilities or assistance".

(c) COMMENCEMENT OF 30-DAY PERIOD AND POSTPONEMENT OF MINIMIZATION.—Section 2518(5) of title 18 of the United States Code is amended—

(1) by inserting after the first sentence the following: "Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered."; and

(2) by adding at the end the following: "In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.".

(d) ALTERNATIVE TO DESIGNATING SPECIFIC FACILITIES FROM WHICH COMMUNICATIONS ARE TO BE INTERCEPTED.—(1) Section 2518(1)(b)(ii) of title of the United States Code is amended by inserting "except as provided in subsection (11)," before "a particular description".

(2) Section 2518(3)(d) of title 18 of the United States Code is amended by inserting "except as provided in subsection (11)," before "there is".

(3) Section 2518 of title 18 of the United States Code is amended by adding at the end the following:

"(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if—

"(i) in the case of an application with respect to the interception of an oral communication—

"(I) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

"(II) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

"(III) the judge finds that such specification is not practical; and

"(ii) in the case of an application with respect to a wire or electronic communication—

"(I) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

"(II) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing of a purpose, on the part of that person, to thwart interception by changing facilities; and

"(III) the judge finds that such purpose has been adequately shown.

"(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11) shall not begin until the facilities from which, or the place where, the communication is to be intercepted is ascertained by the person implementing the interception order.".

(4) Section 2519(1)(b) of title 18, United States Code, is amended by inserting "(including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title did not apply by reason of section 2518(11) of this title)" after "applied for".

SEC. 107. INTELLIGENCE ACTIVITIES.

(a) IN GENERAL.—Nothing in this Act or the amendments made by this Act constitutes authority for the conduct of any intelligence activity.

(b) CERTAIN ACTIVITIES UNDER PROCEDURES APPROVED BY THE ATTORNEY GENERAL.—Nothing in chapter 119 or chapter 121 of title 18, United States Code, shall affect the conduct, by officers or employees of the United States Government in accordance with other applicable Federal law, under procedures approved by the Attorney General of activities intended to—

(1) intercept encrypted or other official communications of United States executive branch entities or United States Government contractors for communications security purposes;

(2) intercept radio communications transmitted between or among foreign powers or agents of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978; or

(3) access an electronic communication system used exclusively by a foreign power or agent of a foreign power as defined by the Foreign Intelligence Surveillance Act of 1978.

SEC. 108. MOBILE TRACKING DEVICES.

(a) IN GENERAL.—Chapter 205 of title 18, United States Code, is amended by adding at the end the following:

"§ 3117. Mobile tracking devices

"(a) IN GENERAL.—If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction.

"(b) DEFINITION.—As used in this section, the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object.".

(b) CLERICAL AMENDMENT.—The table of contents at the beginning of chapter 205 of title 18, United States Code, is amended by adding at the end the following:

"3117. Mobile tracking devices.".

SEC. 109. WARNING SUBJECT OF SURVEILLANCE.

Section 2232 of title 18, United States Code, is amended—

(1) by inserting "(a) PHYSICAL INTERFERENCE WITH SEARCH.—" before "Whoever" the first place it appears;

(2) by inserting "(b) NOTICE OF SEARCH.—" before "Whoever" the second place it appears; and

(3) by adding at the end the following:

"(c) NOTICE OF CERTAIN ELECTRONIC SURVEILLANCE.—Whoever, having knowledge that a Federal investigative or law enforcement officer has been authorized or has applied for authorization under chapter 119 to intercept a wire, oral, or electronic communication, in order to obstruct, impede, or prevent such interception, gives notice or attempts to give notice of the possible interception to any person shall be fined under this title or imprisoned not more than five years, or both.

"Whoever, having knowledge that a Federal officer has been authorized or has applied for authorization to conduct electronic surveillance under the Foreign Intelligence Surveillance Act (50 U.S.C. 1801, et seq.), in order to obstruct, impede, or prevent such activity, gives notice or attempts to give notice of the possible activity to any person shall be fined under this title or imprisoned not more than five years, or both.".

SEC. 110. INJUNCTIVE REMEDY.

(a) IN GENERAL.—Chapter 119 of title 18, United States Code, is amended by adding at the end the following:

"§ 2521. Injunction against illegal interception

"Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.".

(b) CLERICAL AMENDMENT.—The table of sections at the beginning of chapter 119 of title 18, United States Code, is amended by adding at the end thereof the following:

"2521. Injunction against illegal interception."

SEC. 111. EFFECTIVE DATE.

(a) IN GENERAL.—Except as provided in subsection (b), this title and the amendments made by this title shall take effect 90 days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

(b) SPECIAL RULE FOR STATE AUTHORIZATIONS OF INTERCEPTIONS.—Any interception pursuant to section 2516(2) of title 18 of the United States Code which would be valid and lawful without regard to the amendments made by this title shall be valid and lawful notwithstanding such amendments if such interception occurs during the period beginning on the date such amendments take effect and ending on the earlier of—

(1) the day before the date of the taking effect of State law conforming the applicable State statute with chapter 119 of title 18, United States Code, as so amended; or

(2) the date two years after the date of the enactment of this Act.

TITLE II—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

SEC. 201. TITLE 18 AMENDMENT.

Title 18, United States Code, is amended by inserting after chapter 119 the following:

"CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

"Sec.
"2701. Unlawful access to stored communications.
"2702. Disclosure of contents.
"2703. Requirements for governmental access.
"2704. Backup preservation.
"2705. Delayed notice.
"2706. Cost reimbursement.
"2707. Civil action.
"2708. Exclusivity of remedies.
"2709. Counterintelligence access to telephone toll and transactional records.
"2710. Definitions.

"§ 2701. Unlawful access to stored communications

"(a) OFFENSE.—Except as provided in subsection (c) of this section whoever—

"(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

"(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

"(b) PUNISHMENT.—The punishment for an offense under subsection (a) of this section is—

"(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain—

"(A) a fine of not more than $250,000 or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph; and

"(B) a fine under this title or imprisonment for not more than two years, or both, for any subsequent offense under this subparagraph; and

"(2) a fine of not more than $5,000 or imprisonment for not more than six months, or both, in any other case.

"(c) EXCEPTIONS.—Subsection (a) of this section does not apply with respect to conduct authorized—

"(1) by the person or entity providing a wire or electronic communications service;

"(2) by a user of that service with respect to a communication of or intended for that user; or

"(3) in section 2703 or 2704 of this title.

"§ 2702. Disclosure of contents

"(a) PROHIBITIONS.—Except as provided in subsection (b)—

"(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

"(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—

"(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and

"(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

"(b) EXCEPTIONS.—A person or entity may divulge the contents of a communication—

"(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

"(2) as otherwise authorized in section 2516, 2511(2)(a), or 2703 of this title;

"(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

"(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

"(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or

"(6) to a law enforcement agency, if such contents—

"(A) were inadvertently obtained by the service provider; and

"(B) appear to pertain to the commission of a crime.

"§ 2703. Requirements for governmental access

"(a) CONTENTS OF ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a non-voice wire communication or an electronic communication, that is in electronic storage in an electronic communications system for 180 days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than 180 days by the means available under subsection (b) of this section.

"(b) CONTENTS OF ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

"(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or

"(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

"(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena; or

"(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

"(2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service—

"(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

"(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

"(c) RECORDS CONCERNING ELECTRONIC COMMUNICATIONS SERVICE OR REMOTE COMPUTING SERVICE.—A governmental entity may require a provider of electronic communications service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) without required notice to the subscriber or customer if the governmental entity—

"(1) uses an administrative subpoena authorized by a Federal or State statute, or a Federal or State grand jury subpoena;

"(2) obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or

"(3) obtains a court order for such disclosure under subsection (d) of this section.

"(d) REQUIREMENTS FOR COURT ORDER.—A court order for disclosure under subsection (b) or (c) of this section shall issue only if the governmental entity shows that there is reason to believe the contents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State.

"§ 2704. Backup preservation

"(a) BACKUP PRESERVATION.—(1) A governmental entity acting under section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicable consistent with its regular business practices and shall confirm to the governmental entity that such backup copy has been made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

"(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).

"(3) The service provider shall not destroy such backup copy until the later of—

"(A) the delivery of the information; or

"(B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.

"(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than 14 days after the governmental entity's notice to the subscriber or customer if such service provider—

"(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

"(B) has not initiated proceedings to challenge the request of the governmental entity.

"(5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering

with evidence. This determination is not subject to challenge by the subscriber or customer or service provider.

"(b) CUSTOMER CHALLENGES.—(1) Within 14 days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district court or State court. Such motion or application shall contain an affidavit or sworn statement—

"(A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and

"(B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect.

"(2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term 'delivery' has the meaning given that term in the Federal Rules of Civil Procedure.

"(3) If the court finds that the customer has complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the governmental entity's response.

"(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.

"(5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

"§ 2705. Delayed notice

"(a) DELAY OF NOTIFICATION.—(1) A governmental entity acting under section 2703(b) of this title may—

"(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed 90 days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

"(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed 90 days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

"(2) An adverse result for the purposes of paragraph (1) of this subsection is—

"(A) endangering the life or physical safety of an individual;

"(B) flight from prosecution;

"(C) destruction of or tampering with evidence;

"(D) intimidation of potential witnesses; or

"(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

"(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

"(4) Extensions of the delay of notification provided in section 2703 of up to 90 days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) or (c) of this section.

"(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first class mail to, the customer or subscriber a copy of the process or request together with notice that—

"(A) states with reasonable specificity the nature of the law enforcement inquiry; and

"(B) informs such customer or subscriber—

"(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

"(ii) that notification of such customer or subscriber was delayed;

"(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

"(iv) which provision of this chapter allowed such delay.

"(6) As used in this subsection, the term 'supervisory official' means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

"(b) PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS.—A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

"(1) endangering the life or physical safety of an individual;

"(2) flight from prosecution;

"(3) destruction of or tampering with evidence;

"(4) intimidation of potential witnesses; or

"(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

"§ 2706. Cost reimbursement

"(a) PAYMENT.—Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

"(b) AMOUNT.—The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

"(c) The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

"§ 2707. Civil action

"(a) CAUSE OF ACTION.—Any provider of electronic communication service, subscriber, or customer aggrieved by any violation of this chapter in which the conduct

constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity which engaged in that violation such relief as may be appropriate.

"(b) RELIEF.—In a civil action under this section, appropriate relief includes—

"(1) such preliminary and other equitable or declaratory relief as may be appropriate;

"(2) damages under subsection (c); and

"(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

"(c) DAMAGES.—The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000.

"(d) DEFENSE.—A good faith reliance on—

"(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

"(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

"(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense to any civil or criminal action brought under this chapter or any other law.

"(e) LIMITATION.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

"§ 2708. Exclusivity of remedies

"The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.

"§ 2709. Counterintelligence access to telephone toll and transactional records

"(a) DUTY TO PROVIDE.—A Communications common carrier or an electronic communication service provider shall comply with a request made for telephone subscriber information and toll billing records information, or electronic communication transactional records made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

"(b) REQUIRED CERTIFICATION.—The Director of the Federal Bureau of Investigation (or an individual within the Federal Bureau of Investigation designated for this purpose by the Director) may request any such information and records if the Director (or the Director's designee) certifies in writing to the carrier or provider to which the request is made that—

"(1) the information sought is relevant to an authorized foreign counterintelligence investigation; and

"(2) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

"(c) PROHIBITION OF CERTAIN DISCLOSURE.—No communications common carrier or service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

"(d) DISSEMINATION BY BUREAU.—The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

"(e) REQUIREMENT THAT CERTAIN CONGRESSIONAL BODIES BE INFORMED.—On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests made under subsection (b) of this section.

"§ 2710. Definitions for chapter

"As used in this chapter—

"(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

"(2) the term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system.".

(b) CLERICAL AMENDMENT.—The table of chapters at the beginning of part I of title 18, United States Code, is amended by adding at the end the following:

"121. Stored Wire and Electronic Communications and Transactional Records Access ..... 2701".

SEC. 202. EFFECTIVE DATE.

This title and the amendments made by this title shall take effect 90 days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

TITLE III—PEN REGISTERS

SEC. 301. TITLE 18 AMENDMENT.

(a) IN GENERAL.—Title 18 of the United States Code is amended by inserting after chapter 205 the following new chapter:

"CHAPTER 206—PEN REGISTERS

"Sec.
"3121. General prohibition on pen register use; exception.
"3122. Application for an order for a pen register.
"3123. Issuance of an order for a pen register.
"3124. Assistance in installation and use of a pen register.
"3125. Reports concerning pen registers.
"3126. Definitions for chapter.

"§ 3121. General prohibition on pen register use; exception

"(a) IN GENERAL.—Except as provided in this section, no person may install or use a pen register without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

"(b) EXCEPTION.—The prohibition of subsection (a) does not apply with respect to the use of a pen register by a provider of electronic or wire communication service—

"(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

"(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service, or with the consent of the user of that service.

"(c) PENALTY.—Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

"§ 3122. Application for an order for a pen register

"(a) APPLICATION.—(1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

"(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

"(b) CONTENTS OF APPLICATION.—An application under subsection (a) of this section shall include—

"(1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and

"(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

"§ 3123. Issuance of an order for a pen register

"(a) IN GENERAL.—Upon an application made under section 3122 of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register within the jurisdiction of the court if the court finds that the attorney for the government or the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

"(b) CONTENTS OF ORDER.—An order issued under this section—

"(1) shall specify—

"(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register is to be attached;

"(B) the identity, if known, of the person who is the subject of the criminal investigation;

"(C) the number and, if known, physical location of the telephone line to which the pen register is to be attached; and

"(D) a statement of the offense to which the information likely to be obtained by the pen register relates; and

"(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register under section 3124 of this title.

"(c) TIME PERIOD AND EXTENSIONS.—(1) An order issued under this section shall authorize the installation and use of a pen register for a period not to exceed 60 days.

"(2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed 60 days.

"(d) NONDISCLOSURE OF EXISTENCE OF PEN REGISTER.—An order authorizing or approving the installation and use of a pen register shall direct that—

"(1) the order be sealed until otherwise ordered by the court; and

"(2) the person owning or leasing the line to which the pen register is attached, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

"§ 3124. Assistance in installation and use of a pen register

"(a) IN GENERAL.—Upon the request of an attorney for the government or an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in section 3123(b)(2) of this title.

"(b) COMPENSATION.—A provider of wire communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

"§ 3125. Reports concerning pen registers

"The Attorney General shall annually report to Congress on the number of pen register orders applied for by law enforcement agencies of the Department of Justice.

"§ 3126. Definitions for chapter

"As used in this chapter—

"(1) the term 'communications common carrier' has the meaning set forth for the term 'common carrier' in section 3(h) of the Communications Act of 1934 (47 U.S.C. 153(h));

"(2) the term 'wire communication' has the meaning set forth for such term in section 2510 of this title;

"(3) the term 'court of competent jurisdiction' means—

"(A) a district court of the United States (including a magistrate of such a court) or a United States Court of Appeals; or

"(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register;

"(4) the term 'pen register' means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted, with respect to wire communications, on the telephone line to which such device is attached, but such term does not include any device used by a provider of wire communication service for billing, or recording as an incident to billing, for communications services provided by such provider; and

"(5) the term 'attorney for the Government' has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and

"(6) the term 'State' means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.".

(b) CLERICAL AMENDMENT.—The table of chapters for part II of title 18 of the United States Code is amended by inserting after the item relating to chapter 205 the following new item:

"206. Pen Registers ..... 3121".

SEC. 302. EFFECTIVE DATE.

(a) IN GENERAL.—Except as provided in subsection (b), this title and the amendments made by this title shall take effect 90 days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title takes effect.

(b) SPECIAL RULE FOR STATE AUTHORIZATIONS OF INTERCEPTIONS.—Any pen register order or installation which would be valid and lawful without regard to the amendments made by this title shall be valid and lawful notwithstanding such amendments if such order or installation occurs during the period beginning on the date such amendments take effect and ending on the earlier of—

(1) the day before the date of the taking effect of changes in State law required in order to make orders or installations under Federal law as amended by this title; or

(2) the date two years after the date of the enactment of this Act.

PURPOSE

The purpose of the legislation is to amend title 18 of the United States Code to prohibit the interception of certain electronic communications; to provide procedures for interception of electronic communications by federal law enforcement officers; to provide procedures for access to communications records by federal law enforcement officers; to provide procedures for federal law enforcement access to electronically stored communications; and to ease certain procedural requirements for interception of wire communications by federal law enforcement officers.

HISTORY

When the Framers of the Constitution acted to guard against the arbitrary use of government power to maintain surveillance over citizens, there were limited methods of intrusion into the "houses, papers and effects" protected by the Fourth Amendment. During the intervening 200 years, development of new methods of communication and devices for surveillance has expanded dramatically the opportunity for such intrusions.

The telephone is the most obvious example. Its widespread use made it technologically possible to intercept the communications of citizens without entering homes or other private places. When the issue of government wiretapping first came before the Supreme Court in *Olmstead v. United States*, 277 U.S. 438, the Court held that wiretapping did not violate the Fourth Amendment, since

there was no searching, no seizure of anything tangible, and no physical trespass.[1]

But the *Olmstead* case is remembered not only for its holding but for the prescient dissent of Mr. Justice Brandeis, who predicted:

> Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home . . . Can it be that the Constitution affords no protection against such invasions of individual security? [2]

Forty years later, the Supreme Court accepted the logic of Justice Brandeis in *Katz* v. *United States*, 389 U.S. 347 (1967), holding that the Fourth Amendment applies to government interception of a telephone conversation. At the same time, the Court extended Fourth Amendment protection to electronic eavesdropping on oral conversations in *Berger* v. *New York*, 388 U.S. 41 (1967).

Congress responded in a comprehensive fashion by authorizing government interception, under carefully subscribed circumstances, in Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[3] which has come to be known as the Wiretap Act. That legislation protected two common types of communication—telephone conversations and face-to-face oral communications—against electronic eavesdropping. Specifically, the law barred the interception of wire communications over a common carrier unless an appropriate court order had been obtained.[4] Further, it limited the concept of interception to the "aural acquisition" of the contents of a communication.[5] "Oral communications" were protected only in circumstances where there is a reasonable expectation of privacy.[6]

Nature of the Problem

Although it is still not twenty years old, the Wiretap Act was written in different technological and regulatory era. Communications were almost exclusively in the form of transmission of the human voice over common carrier networks. Moreover, the contents of a traditional telephone call disappeared once the words transmitted were spoken and there were no records kept. Consequently the law primarily protects against the aural interception of the human voice over common carrier networks.

The legislation did not attempt to address the interception of text, digital or machine communication.[7] This statutory framework appears to leave unprotected an important sector of the new communications technologies.

Many communications today are carried on or through systems which are not common carriers. Electronic mail, videotex and similar services are not common carrier services. Under existing law

[1] Olmstead v. United States, 277 U.S. 438, 464 (1927). *Compare*, Dow Chemical Co. v. United States, — U.S. — (May 19, 1986) (aerial photography by government without a warrant does not violate Fourth Amendment); California v. Ciraolo, — U.S. — (May 19, 1986) (same).

[2] 277 U.S. at 474 (Brandeis, J., dissenting).

[3] 18 U.S.C. 2510 *et seq.* hereinafter "Wiretap Act."

[4] 18 U.S.C. 2511.

[5] 18 U.S.C. 2510.

[6] *Id.*

[7] Sen. Rep. No. 1097, 90th Cong., 2d Sess. 90, hereinafter "1968 Senate Report."

the interception of these services or the disclosure of the contents of messages over these services are probably not regulated or restricted. Moreover, totally private systems are rapidly being developed by private companies for their own use. It is not uncommon for businesses now not to use the local telephone comapny in some instances the long distance companies in the creation of voice and data networks. Since these networks are private they are not covered by existing Federal law. In addition, data is transmitted over tradional telephone services as well as by these services. Since data, unlike the human voice, cannot be aurally intercepted, it is also largely unregulated and unrestricted under present law.

Today, we have large-scale electronic mail operations, cellular and cordless telephones, paging devices, miniaturized transmitters for radio surveillance, and a dazzling array of digitized information networks which were little more than concepts two decades ago. Unfortunately, the same technologies that hold such promise for the future also enhance the risk that our communications will be intercepted by either private parties or the government.

In 1984 the Federal government engaged in more telephone surveillance and wiretapping than in any year since 1973.[8] Moreover, according to a recent study by the Office of Technology Assessment, Federal agencies are planning to use or already use radio scanners (20 agencies), cellular telephone interception (6 agencies), tracking devices (15 agencies), pen registers (14 agencies), and electronic mail interceptions (6 agencies).[9]

This increased use of a variety of electronic surveillance devices alone is not cause for alarm. There are instances when a particular electronic surveillance technique is justified in a criminal investigation. Congress has recognized this by permitting—under carefully limited circumstance under the Wiretap Act—the tapping of telephone calls or the bugging of rooms. However, despite efforts by both Congress [10] and the courts,[11] legal protection against the unreasonable use of newer surveillance techniques has not kept pace with technology.

The statutory deficiency in Title III with respect to non-voice communications has been criticized by commentators, Congressional experts, and most recently by both the General Accounting Office and the Office of Technology Assessment.[12] The danger is eloquently pointed out by Professor Richard Posner (now United States Circuit Court Judge):

[8] Administrative Office of the United States Courts, *Report on Application for Orders Authorizing or Approving the Interception of Wire or Oral Communications (Wiretap Report) for the Period January 1, 1984 to December 31, 1984.*

[9] Office of Technology Assessment, U.S. Cong., Electronic Surveillance and Civil Liberties (1985), hereinafter "OTA Report."

[10] *E.g.*, The Wiretap Act, *supra* note 3; Foreign Intelligence Surveillance Act, 50 U.S.C. 101 *et seq.*; Right to Financial Privacy Act, 12 U.S.C. 3401 *et seq.*

[11] *E.g.*, United States v. Torres, 751 F.2d 875 (7th Cir. 1984), *cert. den'd*, —U.S.—, 105 S.Ct. 1853 (1985). (court has authority to issue warrant permitting video surveillance); Katz v. United States, 389 U.S., 347 (1967), (Fourth Amendment applies to government wiretapping of telephone conversation); Berger v. New York, 388 U.S. 41 (1967) (Fourth Amendment applies to electronic eavesdropping on oral conversation).

[12] *See generally, Electronic Communications Privacy Act of 1985: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the House Comm. on the Judiciary*, 99th Cong., 1st and 2d Sess.; hereinafter "House Hearings." *See also* Burnham, *Experts Study Effect on Law of Latest Electronic Services*, N.Y. Times, Mar. 18, 1985 (reporting on study by ACLU Project on Privacy and Technology).

> In the absence of market discipline, there is no presumption that the government will strike an appropriate balance between disclosure and confidentiality. And the enormous power of the government makes the potential consequences of its snooping far more ominous than those of . . . a private individual or firm.[13]

This legal uncertainty poses potential problems in a number of areas. First, it may unnecessarily discourage potential customers form using such systems, and encourage unauthorized users to obtain access to communications to which they are not party.[14] Lack of clear standards may also expose law enforcement officers to liability [15] and endanger the admissibility of evidence.[16]

But most important, if Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right.[17] Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances.[18] Additional legal protection is necessary to ensure the continued vitality of the Fourth Amendment.[19]

The Committee believes the bill represents a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement.

Telecommunications Technologies Under Current Law

RADIO TELEPHONES

When Congress passed the Wiretap Act in 1968, most telephone calls were transmitted as they always had been—by wire. Other technologies, however, were already on the horizon, an inevitability implicitly recognized by Congress in protecting telephone calls carried "in whole or in part" over wire. 18 U.S.C. 2510. Today, only a minority of telephone calls are made through wire alone; the majority combine wire with some form of radio technology, usually microwave.

a. Microwave

Microwave consists of extremely high frequency radio waves transmitted point-to-point on line-of-sight paths between antennas located on towers or building tops (in terrestrial microwave systems) and between satellites and earth station "dish" antennas (in satellite-based systems). Like most radio transmissions, the microwave portion of a telephone call is vulnerable to interception.[20]

[13] Posner, *Privacy in the Supreme Court*, 1979 Sup. Ct. Rev. 173, 176 (1979).

[14] House hearings, *supra* note 12 (testimony of P. Walker, P. Quigley, P. Nugent, J. Stanton *et al.*).

[15] *See* Malley v. Briggs, —U.S.— (84-1586, Mar. 5, 1986), 54 U.S.L.W. 4243 (Mar. 5, 1986).

[16] 18 U.S.C. 2515.

[17] According to a recent poll, 77 percent of Americans are concerned about technology's threats to their personal privacy. Louis Harris & Associates, *The Road After 1984*, Southern New England Telephone (1984).

[18] *See* Dow Chemical v. United States, —— US. —— (May 19, 1984) (Powell, J. dissenting).

[19] For recent explorations on the capacity of Congress to interpret the Constitution, *see* Mikva, *How Well Does Congress Support and Defend the Constitution?*, 61 N.C. L. Rev. 587 (1983); Fisher, *Constitutional Interpretation by Members of Congress*, 63 N.C. L. Rev. 707 (1985).

[20] T. Harrington and B. Cooper, The Hidden Signals on Satellite TV (1984).

The equipment to complete an interception can be expensive, and the task difficult; however, the practice is sufficiently well known as to be an option for satellite dish owners and for foreign intelligence agencies. Despite the availability of the technical means of interception of microwave transmissions, such transmissions are protected by the plain language of Title III.

b. Cellular Telephone

In 1981 the Federal Communications Commission approved the use of cellular telephone services.[21] This technology uses both radio transmissions and wire to make "portable" telephone service available in a car, a briefcase, or in rural areas not reached by telephone wire.

In a cellular radiotelephone system, large service areas are divided into honeycomb-shaped segments or "cells"—each of which is equipped with a low-power transmitter or base station which can receive and radiate messages within its parameters. When a caller dials a number on a cellular telephone, a transceiver sends signals over the air on a radio frequency to a cell site. From there the signal travels over phone lines or a microwave to a computerized mobile telephone switching office ("MTSO") or station. The MTSO automatically and inaudibly switches the conversation from one base station and one frequency to another as the portable telephone, typically in a motor vehicle, moves from cell to cell.[22]

Cellular technology, because it is more complex, is more difficult to intercept than traditional mobile telephones; it is, however, more accessible than microwave transmissions. Cellular telephone calls can be intercepted by either sophisticated scanners designed for that purpose, or by regular radio scanners modified to intercept cellular calls.[23]

The availability of this technology poses a troubling conflict between the technology of surveillance and new techniques of communication using radio. Interception of cellular calls is illegal under current federal law.[24] At least one state has passed a law specifically aimed at protecting cellular calls.[25] Notwithstanding

[21] Cellular Communications Systems Decisions, 86 FCC 2d 469 (1981).

[22] House Hearings, *supra* note 12, testimony of P. Quigley, J. Stanton. Cellular technology is more advanced than ordinary mobile telephones. Cell-to-cell "hand-off" of calls maximizes channel capacity, allowing use by many more subscribers in a specific area. In addition, cellular telephone calls are fully automated and do not require the services of a mobile operator.

[23] *House Hearings, supra*, note 12 (testimony of R. Colgan), see Ad, Land Mobile Product. News. Jan. 15, 1985 (for Regency scanners). When cellular service began it was "remarkably private". Huff, *Cellular Phone*, Technology Review, (Nov./Dec. 1983) at 53, 58. This was so because unlike older radio telephones there is usually no operator required to place the calls, and there is no party line function. Greathouse, *Privacy and the Cellular Phone*, Personal Communications Magazine. In addition, because cellular was assigned to new frequencies (between 825 Mhz and 890 Mhz), scanners were not initially available to easily enable scanning of cellular calls by the general public. *Id.* More recently, such scanners have been made available for sale. Hanson, *Legislating Cellular Privacy: An Idea That Won't Work*, Personal Communications Magazine; Corn, *The Privacy Issue*, Cellular Resources, 66, 71 (Sept/Oct 1984); Corn, *The Privacy Issue Updated*, Cellular Resources 46–49 (Nov. 1985).

[24] *See*, House Hearings, *supra* n. 12 (testimony of U.S. Dept. of Just.) (interception of cellular to landline calls illegal because "in whole or in part by wire." 18 U.S.C. 2510); *cf.* United States v. Hall, 488 F.2d 193 (9th Cir. 1973) (same for ordinary mobile telephones); 47 U.S.C. 705 (interception and divulgence or use of communications not broadcast for general public illegal). Perhaps because of the relative newness of the technology, there are no cases directly addressing the issue of cellular interceptions.

[25] Cal. Penal Code §§630 *et seq.*

these legal proscriptions there remains a real-life conflict as interception technology catches up with communications development.[26] The resolution of these competing interests was carefully considered by the Committee.

c. Cordless Telephones

Cordless telephones are another new telephone technology presenting a conflict between communication and interception. A cordless telephone consists of a handset and a base unit wired to a landline and a household/business electrical current. A communication is transmitted from the handset to the base unit by AM or FM radio signals. From the base unit the communication is transmitted over wire, the same as a regular telephone call. The radio portions of these telephone calls can be intercepted with relative ease using standard AM radios.[27]

The legality of intercepting cordless telephone calls has been fully litigated in only two states. The Supreme Courts of Kansas and Rhode Island, both construing federal law, have held that evidence obtained by an interception of a cordless telephone call by law enforcement officials without a warrant can be admitted at trial.[28] In each case the court was convinced that the radio portion of a conversation was entitled to no legal protection against interception.[29] This approach sharply conflicts with the major relevant federal case.[30]

These courts were not required, however, to decide the rights of the other party to the conversations in these cases, persons using conventional landline telephones. While it it possible to argue that a person using a cordless phone knows or has reason to know that the call can be easily overheard, that argument does not apply to the other party to the conversation.

DATA TRANSMISSIONS AND ELECTRONIC MAIL

When Congress enacted the Wiretap Act it specifically excluded the transmission of data from protection against private and governmental interceptions.[31] In the intervening years, data transmission and computer systems have become a pervasive part of the business and home environments.

Computer and telephone technologies have merged; the resulting new communication techniques utilize computer terminals and

[26] House Hearings, *supra* note 12 (testimony of R. Colgan). The wide availability of this technology and its expanded use of up to 7 million such phones by 1990, poses additional challenges to law makers.

[27] *See* State v. DeLaurier, 488 A.2d 688 (R.I. 1985); State v. Howard, 235 Kan. 236, 679 P.2d 297 (1984).

[28] 488 A.2d 688; 235 Kan. 236, 679 P.2d 297.

[29] 488 A.2d 688; 235 Kan. 236, 679 P.2d 297. The state courts concluded that radio communications are neither "wire" nor protected "oral communications". 488 A.2d at 693; 235 Kan. at 247 They reasoned that to require the police to obtain a warrant to listen to an AM radio would be "absurd". 488 A.2d at 694. They also reasoned that such communications were not protected against interception because there is no "reasonable expectation of privacy". State v. DeLaurier, 488 A.2d at 694. State v. Howard, 235 Kan. 236, 676 P.2d 297 (1984). The *DeLaurier* court also found that an AM radio is not a "device" within the meaning of 18 U.S.C. 2510(5), therefore no violation of federal law occurred. 488 A.2d at 694.

[30] United States v. Hall, 488 F.2d 193 (9th Cir. 1973) (interception of radio portion of mobile telephone call violates Wiretap Act since communication "in whole or in part by wire." 18 U.S.C. 2510.

[31] 1968 Senate Report, *supra* note 7, at 90.

video display screens, and frequently transmit data over telephone lines.

The array of services include electronic bulletin boards, electronic data bases, videotext services, and remote computing. Some of these new services permit an individual to use a keyboard and telephone to transmit electronic messages and data and to receive interactive services featuring banking and other financial services, shopping, news, messages, and education. Many of these services also record the nature of the transactions engaged in by the user. Thus, the new technologies represent both an explosion in communication opportunities as well as surveillance possibilities.[32]

One of the most popular new computer services is electronic mail, a service which combines features of the telephone and regular first class mail. Electronic mail can include telex, teletex, facsimile, voice mail and mixed systems that electronically transmit and store messages. Many e-mail users have found it a useful substitute for telephone calls, while others utilize it instead of the government postal service.

Electronic mail differs from regular mail in three ways. First, e-mail is provided by private parties and thus not subject to governmental control or regulation under the postal laws.[33] Second, it is interactive in nature and can involve virtually instantaneous "conversations" more like a telephone call than mail. Finally, e-mail is different from regular mail because the electronic communication provider as part of the service may technically have access to the contents of the message and may retain copies of transmissions.[34]

Any discussion of the application of current law governing interception of e-mail or the use of e-mail surveillance begins with the Fourth Amendment, which protects our reasonable expectation of privacy. There are no reported cases governing the acquisition of e-mail by the government, so an application of the Fourth Amendment to the interception of e-mail is speculative. It appears likely, however, that the courts would find that the parties to an e-mail transmission have a "reasonable expectation of privacy" and that a warrant of some kind is required.

As for statutory protection, while there may be some limits on government access to e-mail messages from an e-mail provider, there do not appear to be any federal statutes which directly address this issue.[35] Title III would not apply, since it is limited to the "aural acquisition" of the contents of a communication, and e-mail usually does not involve the transmission of audible sound.[36] The Communications Act might have some limited application, excepting law enforcement officials.[37] The Foreign Intelligence Sur-

[32] OTA Report, *supra* note 9, at 48.

[33] *See* 18 U.S.C. 1701 *et seq.* These regulations appear to place restrictions on government access to government operated electronic mail systems. Although the United States Postal Service operated an electronic mail system for a short period, that service is no longer in operation.

[34] House Hearings, *supra* note 11 (testimony of P. Walker). E-mail systems are designed to provide access to contents and copies of messages in case of system failure. Messages are electronically generated and not normally accessed by the e-mail provider.

[35] The Right to Financial Privacy Act may apply if certain categories of records are involved. 12 U.S.C. 3401 *et seq.*

[36] *See* 18 U.S.C. 2510; United States v. New York Telephone Company, 434 U.S. 159, 168 (1977).

[37] 47 U.S.C. 705 (which bars the interception and disclosure or use of certain communications) applies only to radio or wire communications. Some courts have held that this statute does not

Continued

veillance Act, however, could be read to require federal law enforcement officials to obtain a court order before engaging in "electronic surveillance" that acquires the contents of e-mail communications.[38] These criminal prohibitions do not apply to private persons.

REMOTE COMPUTING SERVICES

The use of remote computing services has also dramatically increased.[39] Many persons use the facilities of these services to process and store their own data.

A subscriber or customer to a remote computing service transmits records to a third party, a service provider, for the purpose of computer processing. This processing can be done with the customer or subscriber using the facilities of the remote computing service in essentially a time-sharing arrangement, or it can be accomplished by the service provider on the basis of information supplied by the subscriber or customer.

As with electronic mail, remote computing services are still relatively new, and there is no case law directly on point. Proceeding by analogy, under current law a subscriber or customer probably has very limited rights to assert in connection with the disclosure of records held or maintained by remote computing services.[40] It is likely, however, that contents of customer data enjoy a higher degree of Fourth Amendment protection.[41]

PAGING DEVICES

An increasingly important adjunct to the telecommunications systems is the paging system. Radio paging is essentially a one-way message service. Recent estimates indicate that there are over 2.5 million pagers in operation; these numbers are expected to double within five years.[42]

There are three basic types of paging devices: tone-only, digital, and voice.[43] In a tone-only pager system an outside party places a telephone call to the paging service which in turn sends a signal to the user indicating that the user has a telephone call. The user must then call back a specific phone number (often an answering service). The digital or display pager permits the user to receive a

govern the activities of law enforcement officials. United States v. Hall, 488 F.2d 193, 197 (9th Cir. 1973); United States v. Chrisman, 375 F. Supp. 1354 (N.D. Cal. 1974).

[38] 50 U.S.C. 1809(a) provides that it is a felony for a person to "engage in electronic surveillance under color of law except as authorized by statute." 50 U.S.C. 1801(f) includes within the definition of "electronic surveillance" "the acquisition . . . of the contents of any wire or radio communication . . ." 50 U.S.C. 1801(f).

[39] House Hearings, *supra* note 12 (testimony of P. Nugent).

[40] Cf. United States v. Miller, 425 U.S. 435 (1976) (no standing under Fourth Amendment for customer to object to bank disclosure of customer records). Congress reversed the result reached in *Miller* by enacting the Right to Financial Privacy Act, 12 U.S.C. 3401 et. seq.

[41] *Miller*, note 39 *supra*, might be distinguished when contents rather than records are involved. Unlike records of the bank's (or remote computing service's) records, contents are analogous to items stored, under the customer's control, in a safety deposit box.

[42] According to one consultant for Authur D. Little, the number of pagers in service could grow to 10 million (including 6 million display pagers) by 1990. *Telocator Members Told That Paging to Prosper in the Future*, TELOCATOR BULLETIN, September, 1984.

[43] *See generally*, Note, *Does A Part Equal the Whole: Is the Interception of Paging Devices Communications Governed by Title III*, 7 GEO. MASON U.L. REV. 234 (1984). Newer two-way paging devices are apparently on the horizon. Posa, *Radio Pagers Expand Horizons*, HIGH TECHNOLOGY (March, 1983).

digital or alphanumeric message on a display screen. A voice pager permits a person who wishes to communicate with the user to leave a recorded message which is then transmitted to the user. The user actually hears the voice message.

The only reported case on this technology, *Dorsey* v. *State*,[44] involves a voice pager. In the *Dorsey* case, the court upheld the use of a scanner by the police to intercept voice messages transmitted over a paging system to an alleged drug dealer. The court held that these messages are neither wire nor oral communications and, therefore, such interceptions are lawful.[45]

According to the United States Department of Justice, however, the three types of paging devices require different levels of statutory protection.[46] The Department reasons that "tone only" pagers carry no reasonable expectation of privacy and therefore no court order is required for a government official to intercept or monitor such signals. The interception of "display pagers" is, according to the Department of Justice, also not within the ambit of Title III; the Department concedes, however, that because, use of such devices encompasses a reasonable expectation of privacy, governmental interception of messages over such a system requires use of a search warrant under the Fourth Amendment.[47] Finally, the Department of Justice concludes that a "voice pager" is simply the continuation of an original wire communication, and therefore a Title III court order is required.[48]

PEN REGISTERS

The privacy of telephone customers can also be affected by the use of pen registers or other devices which record the numbers dialed from a telephone.[49] Pen registers can be used by telephone companies for internal business purposes[50] as well as by the government for law enforcement purposes.[51] It is this governmental use which has posed the most difficult questions for Congress and the courts.[52]

[44] 402 So. 2d 1178 (Fla. 1981). In *Dorsey*, the Supreme Court of Florida interpreted a state statute *in para lateria* with Federal law. 402 So. 2d at 1183.

[45] *Id.* The *Dorsey* court specifically rejected the reasoning in United States v. Hall, 488 F.2d 193 (9th Cir. 1973).

[46] U.S. Department of Justice, Office of Legal Counsel (Theodore B. Olson), Memorandum for John A. Mintz, Assistant Director-Legal Counsel, Federal Bureau of Investigation, January 5, 1984 (OLSON MEMO).

[47] OLSON MEMO, *Supra* note 40.

[48] *Id. Compare*, Dorsey v. State, 402 So. 2d 1178 (Fla. 1981).

[49] *See* United States v. N.Y. Tel. Co., 434 U.S. 159, 161, 167 (1977); United States v. Giordano, 416 U.S. 505, 549 n. 1 (1974) (Powell, J., concurring in part and dissenting in part).

[50] Telephone companies can use pen registers to verify long distance billing information. Fishman, *Pen Registers and Privacy: Risks, Expectations and the Nullification of Congressional Intent*, 29 CATHOLIC L. REV. 557, 558 (1980). Telephone companies can use pen registers to detect the use of illegal devices, such as "blue boxes." United States v. N.Y. Tel. Co. 434 U.S. 159, 174-75 (1977); *See generally* Note, *The Legal Constraints Upon the Use of the Pen Register as a Law Enforcement Tool*, 60 CORNELL L. REV. 1028, 1029 (1975). Additionally, a pen register could be placed on the phone of a person suspected of placing harrassing or obscene calls. 47 U.S.C. 223. *See generally* Claerout, *The Pen Register*, 20 DRAKE L. REV. 108, 109-110 (1970).

[51] Pen registers are often used to acquire "probable cause" evidence necessary to obtain a search warrant or a Title III wiretap order. HOUSE HEARINGS, *supra* note 12 (testimony of J. Knapp). Remarks, Fred Hess, Criminal Division, United States Department of Justice, Office of Technology Assessment Workshop, May 17, 1985. *See also* Fishman, WIRETAPPING AND EAVESDROPPING 46 (1978).

[52] Slightly different issues are presented when law enforcement officials utilize devices which trap or trace incoming phone calls. Prior to the passage of Title III courts had upheld the use of

Continued

The United States Supreme Court has on two occasions decided cases involving questions about the legality of installation and use of pen registers. *United States* v. *N.Y. Tel. Co.*[53] presented the question whether an ordinary search warrant was sufficient to authorize government use of a pen register. The Court held that the existing federal wiretap law was not implicated by the use of a pen register,[54] and that federal district judges have authority to issue warrants directing telephone company cooperation with the installation of pen registers.[55]

In *Smith* v. *Maryland*[56] the Supreme Court found that law enforcement officials need not obtain a search warrant before securing telephone company cooperation in the installation of a pen register.[57] The Court reasoned that because the person who used the telephone voluntarily disclosed the numbers dialed there was "no reasonable expectation of privacy," eliminating Fourth Amendment protection.[58]

The current practice of federal law enforcement agencies is to obtain a court order, under Rule 57 of the Federal Rules of Criminal Procedures,[59] before using a pen register.[60] This practice conforms with the Foreign Intelligence Surveillance Act,[61] which created a requirement for a court order even in a domestic criminal case.[62] Outside the limited context of foreign intelligence, Congress has specified no standard for obtaining a pen register court order. Thus, current case law and statutes leave federal law enforcement officials with virtually unchecked discretion to obtain information through the use of pen registers. All the government needs to do is make an application to a federal court; no independent judicial review of the facts is required.

RECORDS

Electronic communication technologies have become so pervasive that extensive records are maintained which reveal a great deal about how individuals interact with each other. For decades, telephone companies have maintained telephone toll records and tele-

such devices because of the consent of one of the parties to the communication. Rathun v. United States, 355 U.S. 107 (1957). Enactment of Title III has not affected this result. Carr, The Law of Electronic Surveillance, § 3.03[3] at 84 (1977) and at 23 (1985 Supp.).

[53] 434 U.S. 159 (1977).

[54] *Id. at* 165–68.

[55] *Id. at* 171–78.

[56] 442 U.S. 735 (1979).

[57] *Id.* at 746.

[58] *Id.* at 745.

[59] The Rule specifies: In all cases not provided for by rule, the district judges and magistrates may regulate their practice in any manner not inconsistent with these rules or those of the district in which they act. Fed. R. Crim. Proc. 57.

[60] The Subcommittee on Courts, Civil Liberties and the Administration of Justice of the Committee on the Judiciary, United States House of Representatives, conducted a survey of all 94 federal district court Chief Judges to ascertain how frequently pen registers are used. The Subcommittee received 60 responses which indicated that for those courts 2,199 pen register orders were obtained during the first 9 months of 1985.

[61] Public Law 95–511; 50 U.S.C. 1801 *et seq.*

[62] 50 U.S.C. 1809 creates criminal liability for federal officials who engage in electronic surveillance, unless such official has either a search warrent or a court order from a court of competent jurisdiction. 50 U.S.C. 1801(f) defines "electronic surveillance" to include the acquisition of the "contents" of wire communications, and further defines "contents" to "include any information concerning the identity of the parties to such communication or the existence, substance, purport or meaning of that communication." Thus, the Foreign Intelligence Surveillance Act covers the use of pen registers. H.R. Rep. No. 1293; 95th Cong. 2d Sess. 67 (1978).

graph companies have kept copies of telegrams. There is a body of law which addresses the question of government access to this data.[63] Similarly there are legal rules which limit the access to information about postal correspondence.[64]

The newer technologies such as electronic mail and remote computing services maintain a type of records which do not neatly fit within the legal categories which exist for older technologies. This legal uncertainty has caused concern within the business community for several reasons. First, to the extent that potential customers have less protection when they use an electronic medium than with paper, there may be a disincentive to use an electronic service.[65] Second, if persons with records have a choice of maintaining them "in house" or with a third party, they may be less inclined to go outside if such a move deprives them of legal rights (such as notice and an opportunity to contest government access). Any effort to resolve this legal uncertainty should first proceed from a complete understanding of the existing law with respect to more traditional technologies.

Telephone toll records

As a general matter telephone companies maintain a record of calls placed from a telephone for billing purposes. These business records are primarily used by the telephone company for its own purposes. At the federal level the government can legally obtain access to such records based on a grand jury or trial subpoena or through the use of an administrative summons authorizing a specific federal agency to obtain records.[66] Such government access is usually in connection with an ongoing criminal or civil investigation.[67] The most frequent use of this investigative technique is by the Department of Justice.[68] Requests for telephone toll records would appear to easily exceed 100,000 per year.[69]

At the state level, some states have placed limits on access to telephone toll records by state and local law enforcement. Colora-

[63] *See generally.* Reporters Committee v. AT&T 593 F.2d 1030 (D.C. Cir. 1979) *cert. denied,* 440 N.S. 949 (1979) (no violation of the Fourth Amendment to release toll call records without notice to the customer); *see also* Smith v. Maryland, 442 U.S. 735 (1979) (use of a "pen register is permissible under Fourth Amendment because a subscriber has no reasonable expectation of privacy in numbers dialed.)

[64] 39 U.S.C. 3623(d) (requires search warrant to open first class mail); United States v. Van Leeuwen, 397 U.S. 249 (1970) (first class mail may only be opened pursuant to warrant under Fourth Amendment); Ex parte Jackson, 96 U.S. 727, 733 (1878) ("whilst in the mail . . . [letters] . . . can only be opened and examined under . . . warrant").

The use of mail covers, which record the names and addresses of senders and recipients of mail, have different legal standards applied to their use. Because investigative use of this information does *not* include access to the contents of the lettes there has been a lesser degree of Fourth Amendment concern. *See* note 2, *infra.*

[65] *See* House Hearings, *supra* note 12, testimony of M. Nugent.

[66] Reporters Comm. v. AT&T, *supra* note 61.

[67] *Id.*

[68] *Id.*

[69] The Committee conducted a survey of various telephone companies to ascertain the frequency with which telephone toll records are sought. For approximately six states (Maryland, Washington, D.C., Colorado, Michigan, Illinois and most of California) nearly 10,000 subpoenas were issued by the Department of Justice for a one year time period. NYNEX reported that for New York State alone, subpoenas were received *relating to* between 85,000 and 91,000 telephones per year over the past five years.

In Reporters Comm. v. AT&T, *supra,* note 61, at 1037, it was estimated that the number of requests for telephone toll records was at a rate of between two and three thousand each month.

do,[70] California,[71] Pennsylvania,[72] and New Jersey,[73] have all required that a court order be obtained before access to telephone-created transactional information can be granted. The majority view, however, appears to conform with federal law, that is to permit access based on any form of legal process.[74]

Telegrams

The applicable federal law would appear to permit governmental access to copies of telegrams based on the use of a subpoena.[75]

First class mail searches and mail covers

One of the most frequently used forms of private communication is the government operated first class mail system. Therefore, an assessment of the limitations which have been placed on governmental access to the contents of and/or transactional information concerning first class mail correspondence is relevant to any determination about what legal rights should exist with respect to access by the government to newer forms of communications.

Under current Federal law, a search warrant based on probable cause is required before the government can obtain the contents of a first class letter.[76]

A lower standard is used for government access to mail covers, an investigative technique whereby the postal service records the names and addresses of persons who write to an investigative target or to whom such person writes. While the United States Postal Service does place limits (by regulation) on the use of this technique, courts have thus far declined to find a Fourth Amendment interest implicated by the practice.[77]

STATEMENT

Legislation amending the Wiretap Act to include new technologies, H.R. 214, was first introduced in the 95th Congress by Congressman Robert W. Kastenmeier, Chairman of the Subcommittee on Courts, Civil Liberties and the Administration of Justice of the

[70] People v. Sporleder, 666 p.2d 135 (Sup. Ct. Colo. 1983), Charnes v. diGiacomo, 612 F2d 1717 (Sup. Ct. Colo. 1980), People v. Corr, 682 P.2d 20 (Sup. Ct. Colo. 1984).

[71] People v. Blair, 25 Cal. 3d 640, 602 P.2d 738 (Calif. Sup. Ct. 1979); People v. McKunes, 124 Cal. Rep. 126 (Calif. Ct. App. 1975).

[72] Commonwealth v. DeJohn, 986 Pa. 32, 403 A.2d 1283 (1979), *Cert. denied*, 444 U.S. 704 (1980).

[73] State v. Hunt, 91 N.J. 338, 450 A.2d 952 (1982); Note, 13 Seton Hall L. Rev. 803 (1983).

[74] In re Order for Indiana Bell Telephone to Disclose Records 409 N.E. 2d 1069 (Sup. Ct. Ind. 1980); State v. Fredette, 411 A.2d 65 (Sup. Ct. Me. 1979); Hastetter v. Behan, 639 p.2d 10 (Sup. Ct. Montana. 1982); People v. DiRaffaele, 55 N.Y. 2d. 234, 432 N.E. 513 (Ct App. 1981); Fitzgerald v. State, 599 p.2d 572, 577 (Sup. Ct. Wyo. 1979).

[75] Wheeler v. United States, 226 U.S. 478 (1913) (a subpoena requiring production of telegrams upheld against a Fourth Amendment challenge); *see also* Brown v. United States, 276 U.S. 134 (1928) (upholding finding of criminal contempt against person who refused to comply with subpoena of copies of telegrams).

[76] *See* note 62, *supra*.

[77] 39 C.F.R. 233.2; United States v. Krauth, 769 F.2d 473 (8th Cir. 1985) United States v. Gering, 716 F.2d 615 (9th Cir. 1983); United States v. Depoll, 628 F.2d 779 (1980); United States v. Huie, 593 F.2d 14 (5th Cir. 1979); United States v. Choate, 576 F.2d 165 (1978); and 619 F.2d 11 (9th Cir. 1980); Vreeden v. David, 718 F.2d 343 (10th Cir. 1983); *see also* Paton v. LaPrade, 469 F.Supp. 773 (D.N.J. 1978). See generally Burnham, *Keeping an Eye on Suspect Mail, New York Times*, March 1, 1986, pg. B-10.

House Committee on the Judiciary. That legislation grew out of widespread general concern with government surveillance.[78]

Although H.R. 214 was not enacted, Congressman Kastenmeier revisited the subject in general oversight hearings held in the 98th Congress entitled "1984: Civil Liberties and the National Security State." [79]

As a result of those hearings, a bill, H.R. 6343, was introduced in the 98th Congress by Congressman Kastenmeier that served as a model for legislation in the 99th Congress.

During the 99th Congress, the Committee, acting through the subcommittee on Courts, Civil Liberties, and the Administration of Justice—held four days of hearings on H.R. 3378 the bill on which H.R. 4952 is based, introduced by Chairman Kastenmeier and Cong. Carlos J. Moorhead, ranking minority Member of the Subcommittee. An identical bill, S. 1667, was introduced in the Senate by Sen. Patrick J. Leahy, ranking minority Member of the Subcommittee on Patents, Copyrights and Trademarks of the Senate Committee on the Judiciary, and Sen. Charles McC. Mathias, Chairman of the Subcommittee .

On September 26, 1985, the Subcommittee heard from the following witnesses: Senator Patrick Leahy (United States Senator from Vermont); Philip M. Walker (general regulatory counsel, GTE Telenet Inc., on behalf of the Electronic Mail Association); and Philip J. Quigley (president and chief executive officer, Pactel Mobile Companies, on behalf of the Cellular Telecommunications Industry Association).

On October 24, 1985, the subcommittee heard from Fred W. Weingarten (program manager, communication and technologies program, Office of Technology Assessment, United States Congress); P. Michael Nugent (government affairs counsel, Electronic Data Systems Corporation, on behalf of ADAPSO, the computer software and services industry association); and John Stanton (executive vice president, McCaw Communications Companies, Inc., on behalf of Telocator Network of America).

On January 30, 1986, the subcommittee took testimony from Neal Amick (division manager for corporate security, American Telephone and Telegraph Company); John W. Kelly Jr. (attorney, Southwestern Bell Telephone Company); Perry Williams (secretary, American Radio Relay League, Inc., a group representing ham radio operators, presenting the statement of Dr. Larry E. Price, president of the group); George A. Kuhnreich, (vice president for corporate planning and governmental affairs, Tandy Corporation); and Richard T. Colgan (executive secretary, Association of North American Radio Clubs).

On March 5, 1986, the final day of hearings, the witnesses were James I. K. Knapp (Deputy Assistant Attorney General, Criminal Division, United States Department of Justice); and Clifford F. Fishman (Professor of Law, Columbus School of Law, Catholic University of America, and author of *Wiretapping and Eavesdropping.*

[78] *See generally Surveillance: Hearings on the Matter of Wiretapping, Electronic Eavesdropping, and Other Surveillance Before the Subcommittee on Courts, Civil Liberties and the Administration of Justice of the House Comm. on the Judiciary*, 94th Cong., 1st Sess.

[79] *1984: Civil Liberties and the National Security State: Hearings Before the Subcommittee on Courts, Civil Liberties and the Administration of Justice*, 98th Cong., 1st and 2d Sess. 133–258.

The Subcommittee took note that the Senate held a hearing on S. 1667, on November 13, 1985.

After completion of the hearing process in the 99th Congress, H.R. 3378, the bill on which H.R. 4952 is based, went to subcommittee mark-up on May 14, 1986. Two amendments, offered by Mr. DeWine, were not accepted by the subcommittee. A quorum of Members being present, the bill, as amended by Chairman Kastenmeier by an amendment in the nature of a substitute, was passed by a voice vote and reported in the form of a clean bill. H.R. 4952 was introduced by Mr. Kastenmeier on June 5, 1986, cosponsored by 14 Members of the subcommittee and 10 other Members: Mr. Moorhead, Mr. Brooks, Mr. Mazzoli, Mr. Synar, Mrs. Schroeder, Mr. Frank, Mr. Morrison of Connecticut, Mr. Berman, Mr. Bouncher, Mr. Hyde, Mr. Kindness, Mr. Swindall, Mr. Coble, Mr. Edwards of California, Mr. Conyers, Mr. English, Mr. Matsui, Mr. Bruce, Mr. Owens, Mr. Mitchell, Mr. Kostmayer, Mr. Nowak, and Mr. Leland.

On June 10, 1986, the full Committee considered H.R. 4952 and, after general debate, and without substantive amendment, ordered the bill reported favorably by roll call vote, 34–0, a quorum of Members being present.

Support for the Legislation

The organizations and individual corporations named below support the principles embodied in the legislation.

Organizations

Electronic Mail Association
ADAPSO (Computer software and services industry association)
Telocator Network of America
Cellular Telecommunications Industry Association (CTIA)
American Civil Liberties Union (ACLU)
National Association of Manufacturers (NAM)
U.S. Chamber of Commerce
National Association of Broadcasters (NAB)
National Cable Television Association (NCTA)
National Association of Business & Educational Radio (NABER)
American Radio Relay League (ham operators)
CBEMA (Computer and Business Equipment Manufacturers Association)
U.S. Telephone Association
Videotext Industry Association
Information Industry Association
Electronic Funds Transfer Association
Radio and Television News Directors Association
Association of American Railroads
Institute of Electrical and Electronics Engineers (IEEE)
Direct Marketing Association
Utilities Telecommunications Council
Associated Credit Bureaus, Inc.

Corporations

AT&T
General Electric
IBM
GTE
ITT
MCI
CBS
Capital Cities/ABC, Inc.
National Broadcasting Co., Inc. (NBC)
Tandy Corporation (Radio Shack)
EDS, a subsidiary of General Motors Trintex
Equifax
TRW
Source Telecomputing Corporation
Chase Manhattan Bank
Motorola
Ameritech
Bell Atlantic
Bell South
Southwestern Bell
NYNEX
Pacific Telesis
US West
Associated Credit Services, Inc.

Agency Views

U.S. Department of Justice,
Office of Legislative and Intergovernmental Affairs,
Washington, DC, June 6, 1986.

Hon. Peter Rodino, Jr.,
Chairman, Committee on the Judiciary,
House of Representatives, Washington, DC.

Dear Mr. Chairman: This letter is to advise you of the Department of Justice's position with regard to H.R. 4952, the Electronic Communications Privacy Act of 1986, which we understand is scheduled for markup on June 10 by the full House Judiciary Committee. This bill makes important changes to the existing wiretap statutes and fills gaps in current laws by creating provisions to regulate interception of and access to new forms of electronic communication such as data transmissions.

The Department of Justice has worked intensively on this legislation over the past several weeks with the members and staff of the Subcommittee on Courts, Civil Liberties and the Administration of Justice, as well as with interested representatives of industry and civil liberties groups. While initial versions of this legislation did not in our view adequately safeguard legitimate and vital law enforcement and national security needs for access to communications, as a result of the negotiations that have occurred the bill has been substantially modified to accommodate our concerns. In our judgment the bill as presently drafted fairly balances the interests of privacy and law enforcement and its enactment would represent a major accomplishment of the 99th Congress, holding forth the promise of significant benefits for business, privacy, and law enforcement alike.

Accordingly, the Department of Justice strongly supports the enactment of H.R. 4952.

Sincerely,

JOHN R. BOLTON,
Assistant Attorney General.

SECTION-BY-SECTION ANALYSIS

Section 1 provides the short title for the bill, the Electronic Communications Privacy Act of 1986.

TITLE I—INTERCEPTION OF COMMUNICATIONS AND RELATED MATTERS

Section 101 contains five subsections. Subsection (a) contains the definitions, and amendments to definitions, used in this chapter and in the new chapter 121 of title 18.

Subsection (a)(1) contains three subparagraphs. Subsection (a)(1)(A) amends the definition of "wire communication" to include aural transfers. The term "aural transfer" is defined in section 2510 (18) of this title. The term "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and point of interception. Thus, the amended definition is intended to encompass existing telephone services.[80] Digitized voice communications are included to the extent that the communication originates with human voice. As a result of this change, a company whose activities affect interstate commerce and which installs its own private telephone or electronic communication system would have that system covered by the statute.

By amending the definition of "wire communication" in subsection (a)(1)(8) to include communications utilizing wires, cables, or other like connections within a switching office, the Committee intends that "wire communication" be construed to include communications made over cellular systems (as defined in 47 C.F.R. § 22.2),[81] regardless of whether the communications are between two cellular telephones or between a cellular telephone and a "landline" telephone.

Existing law, which prohibits interception of wire communications or oral communications, was enacted prior to the development of cellular telecommunications and does not provide adequate privacy protection to conversations transmitted over a cellular system. The Department of Justice has taken the position that, under existing law, communications between a mobile radio telephone and a landline telephone are wire communications, but that conversations between two radio telephones and not carried in whole or in part by regular telephone lines are neither wire communications nor oral communications. Inasmuch as all cellular communications (whether mobile-to-mobile or mobile-to-landline) must pass through a mobile telephone switching office, the Committee bill will remedy this inadequacy and provide explicit privacy protection to all communications utilizing cellular radio.

[80] The term "other like connection" as used in section 2510(1) includes fiber optic cable.

[81] *Cellular System.* A high capacity land mobile system in which assigned spectrum is divided into discrete channels which are assigned in groups to geographic cells covering a geographic service area. The discrete channels are capable of being reused in different cells within the service area.

In the event that the evolution of cellular technology permits the switching or transmission of mobile-to-mobile service (or mobile-to-landline service) without the use of wire, cable, or other like connection, the Committee intends that cellular communications be included within the term "electronic communication". Because cellular communication is transmitted over a communication system currently regarded by the FCC as a common carrier,[82] the Committee also intends that such communication not be considered "readily accessible to the general public" at any time subsequent to the date of enactment, regardless of how a provider of cellular service is denominated by any state or how the FCC may classify any such provider in the future.

The Committee's intention of providing privacy protection to cellular communications in any event is also reflected in the specific inclusion in the legislation of penalties for the interception of such communications.[83]

Part of the impetus to clarify the illegality of interception of cellular communications has been provided by the advertisement of scanning receivers (popularly known as "scanners") specifically promoting eavesdropping on conversations transmitted over cellular systems. Apparently after the FCC allocated frequencies to cellular radio some manufacturers of scanners added the capability to stop at and receive signals transmitted on these frequencies. The Committee finds this development troubling, and expects that the future design and manufacture of scanners will take into account the privacy protections accorded cellular telephony in this legislation.

Section 101(a)(1) amends the definition of "wire communication" to include "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection * * * furnished or operated by any person engaged in providing or operating such facilities for the transmission of * * * *communications affecting interstate or foreign commerce* * * *." Similarly, section 101(a)(5) defines a new term "electronic communication" to include "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a * * * *system that affects interstate or foreign commerce* * * *."

By the inclusion of the element "affecting (affects) interstate or foreign commerce" in these provisions the Committee does not intend that the Act regulate activities conducted outside the territorial United States. Thus, insofar as the Act regulates the "interception" of communications, for example, it, like the Omnibus Crime Control and Safe Streets Act of 1968, regulates only those "interceptions" conducted within the territorial United States. *See Stowe* v. *Devoy*, 588 F.2d 336 (2d Cir. 1978), *cert. denied*, 442 U.S. 931 (1979), and cases cited therein. *See also Berlin Democratic Club* v. *Rumsfield*, 410 F.Supp. 144, 157 (D.D.C. 1976), *United States* v. *Toscanino*, 500 F.*2d* 267, 279–280 (2d Cir. 1974); *Unites States* v. *Cotroni*, 527 F.2d 708 (2d Cir. 1975). Similarly, the controls in section 201 of the Act regarding access to stored wire and electronic com-

[82] *See* Cellular Communications Systems, 86 FCC 2d 469, 496 (1981).

[83] *See* 18 U.S.C. § 2511(4)(b), *as added by* § 101(d)(2) of H.R. 4952.

munications are intended to apply only to access within the territorial United States.

Subsection (a)(1)(C) amends the definition of wire communication to delete the "common carrier" requirement. In the current environment, numerous entities provide electronic communications services beyond the traditional common carrier. Therefore, the Committee chose to extend federal jurisdiction to the maximum permissible constitutional limits by providing coverage of a person who provides or operates facilities for communications that affect interstate or foreign commerce. *See Heart of Atlanta Motel* v. *United States, 379 U.S. 241, 258-259 (1964).*

In the present telecommunications environment, a terminating or originating customer or subscriber will often have installed his own facilities to switch or otherwise process his incoming or outgoing traffic. One example of such equipment is the "private branch exchange", or PBX, typically owned or leased by the customer and located on his premises, and used to interconnect the customer's telephones and date terminals with one another and with the lines of the local exchange carrier, one or more interexchange carriers, and possibly other service providers. To the extent that electronic and wire communications passing through PBXs and other such equipment affect interstate commerce, the Committee intends that those communications tbe protected under Section 2511. The interception of an electronic or wire communication at a point on the customer's premises is thus as much a violation of Section 2511 as if the interception were made through the equipment of a communications carrier. Similarly, where a user has interconnected its own equipment into a private network, communications carried on the network are fully entitled to the protections of Section 2511.

Subsection (a)(1)(D) amends the definition of wire communication to exclude the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit.

By "cordless telephone" we refer *not* to a cellular telephone, but to the type of telephone which uses a short range (a few hundred feet) radio link between the handset and the base unit in place of the usual wire. Such telephones are regulated under Part 15, subpart E of the rules of the Federal Communications Commission (FCC), and are not licensed. Because the communications made on some cordless telephones can easily be intercepted with readily available technologies (such as AM radio), it would be inappropriate to make such interception a criminal offense. The absence of privacy protection has been noted by the FCC. 47 C.F.R. § 15.236(a) (requiring a label stating "PRIVACY OF COMMUNICATIONS MAY NOT BE ENSURED WHEN USING THIS PHONE"). This view also comports with some recent cases. *See* discussion of current law, *supra*. It should be noted that it is only the *radio portion* of the communication that is excluded. The wire portion of the communication remains fully covered in the same sense as a traditional wire telephone conversation.

Subsection (a)(2) amends the definition of oral communication to exclude electronic communications. An oral communication is an utterance by a person under circumstances exhibiting an expectation that the communication is not subject to interception, under

circumstances justifying such an expectation. In essence, an oral communication is one carried by sound waves, rather than by an electronic medium.

The definitions of wire communication and oral communication are not mutually exclusive. Accordingly, different aspects of the same communication might be differently characterized. For example, a person who overhears one end of a telephone conversation by listening in on the oral utterances of one of the parties is intercepting an oral communication. If the eavesdropper instead taps into the telephone wire, he is intercepting a wire communication. There have been cases involving radio communications in which the court having determined that the radio communication was not a wire communication then analyzes it in privacy terms to determine if it is an oral communication. The Committee views this as an inappropriate consideration and the amendment to 18 U.S.C. 2510(2) rejects that case analysis. *See, e.g.; United States v. Rose,* 669 F.2d 23 (1st Cir. 1982).

Subsection (a)(3) amends section 2510(4) of title 18 to provide a definition for the term "intercept" with respect to electronic communications. The definition under current law of "intercept" is retained with respect to "wire" and "oral communications" with one exception. The Committee added the term "or other" after "aural". This change is intended to make clear that it is illegal to intercept the non-voice portion of a wire communication such as the data or digitized portion of a voice communication. The term intercept with respect to "electronic communications" is defined to mean "the interception of the contents of that communication through the use of any electronic, mechanical or other device".

Subsection (a)(4) amends section 2510(3) to strike the words "identity of the parties to such communication or the existence". This amendment avoids any ambiguity about the legality of the use of "pen registers". The Supreme Court has clearly indicated that the use of pen registers does not violate either this chapter or the Fourth Amendment. This amendment makes that policy clear. In addition, this amendment should be read in conjunction with the new chapter on pen registers, chapter 206 of title 18. It does not, however, affect the installation on use of pen registers under the Foreign Intelligence Surveillance Act. 50 U.S.C. 1801 *et. seq.* This amendment also makes clear the distinction between contents of communications and transactional records. The omission of a conforming amendment to the definition of "contents" in section 705 of title 47 is not intended to affect the current law under that section with respect to pen registers. The use of pen registers has been found not to violate section 705. *See Hodge* v. *Mountains Tel. & Telegraph Co.,* 555 F.2d 254 (19th Cir. 1977).

Subsection (a)(5) adds six new definitions to the chapter. Section 2510 is amended by adding a new subsection (12) to define "electronic communications". This expansion permits the inclusion in the general wiretapping and bugging law of many new forms of communication. For example, digitized transmissions and electronic mail will be provided with protection against interception. The definition of electronic communication means "any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electro-

magnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include any wire or oral communication." Excluded from the definition of "electronic communication" are: (1) the radio portion of a cordless telephone communication; (2) any wire or oral communication; (3) any communication by a tone-only paging device; or (4) any communication from a tracking device.

The term "electronic communication" is intended to cover a broad range of communication activities that affect interstate or foreign commerce, except that the term does not include either oral or wire communications. As a rule, a communication is an electronic communication if it is neither carried by sound waves nor can fairly be characterized as one containing the human voice (carried in part by wire). Communications consisting solely of data, for example, and all communications transmitted only by radio would be electronic communications.

A wire communication encompasses the whole of a voice telephone transmission even if part of the transmission is carried by fibre-optic cable or by radio—as in the case of cellular telephones and long-distance satellite or microwave facilities. This result is generally in accord with the case law. *See United States* v. *Clegg*, 509 F.2d 605, 611 (5th Cir. 1975); *United States* v. *Gregg*, 629 F. Supp. 958, 963 (W.D. Mo. 1986). Moreover, the conversion of a voice signal to digital form for purposes of transmission does not, in itself, render the communication non-wire; the provider's choice of transmission technology should not be dispositive. The Committee has intentionally omitted from the definitions any indication that a wire communication cannot also exhibit some of the characteristics of an electronic communication.

It should be noted that an improperly mechanical reading of the phrase "in whole or in part * * * by the aid of wire * * *" could sweep in virtually all voice communications made with the aid of any electronic equipment, inasmuch as virtually all such equipment includes in its assembly some length of wire or the equivalent. The Committee, however, intends the quoted phrase to refer to wire that carries the communication to a significant extent from the point of origin to the point of receipt, and not to wire that is found inside the terminal equipment at either end of the communication. On the other hand, communications over a length of wire that connects two telephones in the same building would be protected as wire communications. Similarly a cellular telephone system which uses either the wire-line system or wires in a switching station is covered as a wire communication.

A transaction may consist, in parts, of both electronic communications and wire or oral communications. For example, the transmission of data over the telephone is an electronic communication; but if the parties used the line to speak with one another between data transmissions, they would then be making a wire communication. And, indeed, a party's utterances into the telephone mouthpiece are an oral communication. The rules governing interception or disclosure may be different for each type of communication. The Committee understands that the Department of Justice will apply for a court order under the "wire" standards in cases where a tap may intercept mixed wire and electronic communications. As long

as the wire standards are followed a single court order should suffice to authorize the interception of both wire and electronic communications involving the same lines or instruments.

Inclusion of the term "radio" in the definition of "electronic communication" in Section 2510(12) reflects the fact that radio communications come within the scope of chapter 119. A number of other provisions, however, affect the legality of the interception of radio communications under chapter 119. The Committee does not intend any of the provisions directed specifically to radio to affect the applicability of Section 705 of the Communications Act of 1934, as amended, to actions by members of the public.

Subsection (a)(5) also adds a definition for the term "user." "User" means any person or entity who uses an electronic communication service and is duly authorized by the provider of such service to engage in such use.

Interception of closed circuit television communications is only included in the bill in a limited fashion. If a person or entity transmits a closed circuit television picture of a meeting using wires, microwaves or other method of transmission, the transmission itself would be an electronic communication and interception of the picture at any point without either consent or a court order would be in violation of the statute. By contrast, if law enforcement officials were to install their own cameras and create their own closed circuit television picture of a meeting, the capture of the video images would not be an interception under the statute because there would be no interception of the contents of an electronic communication. This would be so even if the law enforcement agency utilized the wiring in the premises to insall the cameras and transmit the images. Intercepting the audio portion of the meeting would of course be an interception of an oral communication and the statute would apply to that portion.

Under the Fourth Amendment and recent case law in the area, law enforcement authorities are bound to seek a court order based on probable cause to place a closed circuit television camera in premises where there is a reasonable expectation of privacy without at least one party consent. The whole area of closed circuit television is suitable for Congressional action and is a likely subject of legislation in the future. *See* H.R. 3455 (Kastenmeier) (applying Title III standards to video surveillance) The Committee is aware that the Department of Justice follows the rules established by the leading cases in this area in seeking closed circuit television orders,[64] and the Committee believes this is a wise procedure pending either legislation on the subject or a final judicial resolution of these issues.

Subsection (a)(5) also adds a new definition for "electronic communication system" to mean any wire, radio, electronic photoelectronic or photooptical facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.

Subsection (a)(5) adds a definition for "electronic communication service" to mean any service which provides to users thereof the

[64] United States v. Torres, 751 F.2d 875 (7th Cir. 1984); see also *United States* v. *Brasuci*, 786 F. 2d 504 (2d Cir. 1986).

ability to send or receive electronic communications or wire communications. These services can be provided through the same facilities. Common carriers like existing telephone companies are deemed providers of an electronic communication service.

Subsection (a)(5) adds a definition for the term "readily accessible to the general public." This term is used in section 2511(2) which creates an exception to the general prohibitions on interception. The new paragraph (16) states "readily accessible to the general public" means with respect to a radio communication, that such is not in one of five separate categories. In other words, if a radio communication fits into one of the five categories then it will have privacy protection (unless some other exception applies to preclude coverage). The first category of protected communications [55] is radio communications which are scrambled or encrypted. The terms scrambled or encrypted are used in their technical sense. To "Encrypt" or to "Scramble" means to convert plaintext into unintelligible form by means of equipment intended to protect the contents of a communication from unintended recipients. Equipment which merely changes the form of a plaintext message, e.g., a device which converts an analog signal to a digital stream, does not provide "encryption" within the meaning of this bill. The use of a word code, no matter how sophisticated, would not suffice. Examples of scrambling techniques which are currently available include the data encryption standard (DES).

The second type of protected communications is spread spectrum radio communications. These radio signals are transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication. *See* 50 FED. REG. 25234 (June 18, 1985). Spread spectrum technology usually involves the transmission of a signal on different frequencies and the receiving station must possess the necessary algorithm in order to reassemble the signal.

The third type of protected communications is radio communications carried on a subcarrier or other signal subsidiary. This category includes, for example, data and background music services carried on FM subcarriers and data carried on the vertical blanking interval (VBI) of a television signal. Under Section 2511(2)(g)(ii)(I), however, it is not unlawful to intercept subcarrier and VBI communications that are transmitted for the use of the general public, *e.g.*, the stereo subcarrier used in FM broadcasting, or data carried on the VBI to provide closed-captioning of television programming for the hearing-impaired.

The fourth type of protected communications is those which are carried by common carriers. There is an exception for tone-only paging systems. Thus, the interception of tone-only paging system transmissions will not be prohibited by this law. On the other hand, the unauthorized interception of a displaying paging signal intended for digital display by the paging receiver (which involves the transmission of alphanumeric characters over the radio) carried by a common carrier is illegal.

[55] Protected communication as used in this description means that the communication is otherwise legally protected against interception absent the application of some other exception such as one party consent.

The fifth type of protected communications consists of certain types of radio signals. Included in this category are satellite communications, auxiliary broadcast services and private microwave services. Each of these services routinely carries business or personal communications made with an expectation of privacy. These categories are described by reference to certain parts of the Rules of the Federal Communications Commission. This category excludes certain communications which are essentially two-way voice radio communications.

Part 25 of the FCC's Rules regulates communications made by satellite. Such communications are not defined to be readily accessible to the general public. Two other provisions of this Act, however, limit the liability incurred under chapter 119 by the interception of certain types of satellite communications. Section 2511(g)(iii)(II) exempts activities covered by section 705(b) of the Communications Act, relating to the interception or receipt of certain satellite cable programming for private viewing; accordingly, such activities are not unlawful under chapter 119. Section 2511(4)(b)(iii) further provides that it is not an offense under Section 2511(4) to intercept an unscrambled and unencrypted "network feed"—*i.e.*, a satellite transmission that is transmitted to a broadcasting station for purposes of retransmission to the general public—so long as the conduct is not for the purposes of direct or indirect commercial advantage or private financial gain.

Also excluded from the category of readily accessible radio communications are those transmitted on frequencies allocated under subparts D, E, and F of Part 74 of the FCC's Rules. Under the FCC's Rules, these frequencies may be licensed only to broadcasters. 47 C.F.R. §§ 74.432, 74.532, 74.632. Each of the subparts regulates communications that are entirely internal to a broadcast operation. They include, for example, video and audio transmissions from a news team in the field to the studio, and transmission from the studio to the transmitter site. Part 74 transmissions may also include two-way voice communications, such as those between studios and remote crews; but this Act provides an exception for such two-way voice communications made on frequencies shared with services outside Part 74. The interception of communications on such shared frequencies is not unlawful under chapter 119.

The final service excluded from the category of readily accessible radio communications is that regulated under Part 94 of the FCC's Rules, the private operational fixed microwave service. This service carries confidential business data. Under limited conditions, it may also be used to transmit certain types of television material. Transmissions under Part 94 are generally made with the intent of maintaining privacy, and it would be inappropriate to disrupt ongoing business practices by making those communications available to competitors and to other members of the public.

Subsection (a)(5) also provides a definition for "electronic storage". That terms means "any temporary intermediate storage of a communication incidental to the electronic transmission thereof and any storage of such communication by an electronic communication service for purposes of backup protection of such communication." Section 2510(17) defines "electronic storage" to mean any temporary, intermediate storage of a communication incidental to

the electronic transmission thereof, and any storage of such communication by an electronic communication service for purposes of backup protection of such communication. Under Section 2710, computer storage is defined as an element of "remote computing service". These definitions are not intended to limit the terms "electronic storage" or "computer storage" to any particular medium of storage. While storage often takes place within the random access memory of a computer, the term applies equally to storage in any other form, including that on magnetic tape, disks, or other media. Thus, for example, the prohibitions against unauthorized access to a wire or electronic communication while it is in electronic storage, as set forth in Section 2701, would prohibit unauthorized access to such a communication while it is stored on magnetic tape or disk. The prohibitions would apply similarly to information held on magnetic tape or disk pursuant to an agreement to provide remote computing service.

Subsection (a)(5) adds a new definition for the term "aural transfer". "Aural transfer" means a "transfer containing the human voice at any point between and including the point of origin and the point of reception". Under this definition voice messages transferred over a paging system are protected. It is intended that computer-generated or otherwise artificial voices are not included in this definition and thus will not be part of a "wire communication". They would, however, be part of an "electronic communication".

Subsection 101(b) makes three different types of amendments to existing title 18.

Subsection (b)(1) amends section 2511(2)(d) of title 18 by striking out "or for the purpose of committing any other injurious act". Under current federal law it is permissible for one party to consent to the interception and recording of a conversation. This exception to the general prohibition on interception, however, contains an exception relating to persons who intercept or record communications for illegal, tortious or other injurious purposes. This exception was added in 1968 by the late Senator Hart in an effort to prevent one party from intercepting or recording a conversation for blackmail or similar improper purposes. Unfortunately, that floor amendment was not drafted with precision. As a result, numerous court cases have arisen wherein the term "other injurious purposes" has been construed and misconstrued. Most troubling of these cases have been attempts by parties to chill the exercise of First Amendment rights through the use of civil remedies under this chapter. For example, in *Boddie* v. *American Broadcasting Co.*, 731 F.2d 333 (6th Cir. 1984), the plaintiff, whose conversations were recorded by a journalist, sued. Despite the consent of the reporter who was a party to the conversation, the plaintiff claimed that the recordation was illegal because it was done for an improper purpose (e.g., to embarrass the plaintiff). The court's opinion suggests that if the network intended to cause "insult and injury" to plaintiff Boddie, she might be entitled to recover. This interpretation of the statute places a stumbling block in the path of even the most scrupulous journalist. Many news stories have been brought to light by recording a conversation with the consent of only one of the parties involved—often the journalist himself. Unfortunately, many news

stories are embarrassing to someone. The present form of the statute not only provides such a person with a right to bring suit, but it also makes the actions of the journalist potentially a criminal offense under section 2511, even if the interception was made for the purpose of committing neither a criminal act nor a tort. The statute thus presents the journalist with a hard choice: to get the news may expose him or her to a criminal conviction and/or civil liability. And whether a journalist is convicted in fact may turn, under *Boddie,* on how a jury sitting years later assesses the journalist's subjective intent. The Committee finds such a threat to be inconsistent with the guarantees of the First Amendment. Inasmuch as the amended statute continues to prohibit interceptions made for the purpose of committing either a crime or a tort (including acts of defamation), the Committee believes that the public will be afforded ample protection against improper or unscrupulous interception. The amendment is intended to remove only the shadow of a finding that section 2511 has been violated by interceptions made in the course of otherwise responsible news gathering. While the appeals court decision merely sent the case back for further factual development, it is clear from the facts of the case that the term "improper purpose" is overly broad and vague. The deletion of the term leaves in place the exception to one party consent for illegal or tortious interceptions or recordation. Thus, the original purpose of the Hart amendment is preserved without maintenance of the litigation-breeding phrase. This amendment is supported by the Department of Justice.

Subsection (b)(2) amends section 2511(2)(f) to expand the exception applicable to foreign intelligence activities to make sure the provisions of chapter 121 do not adversely affect such activities.

Section 101(b)(2) of H.R. 4952 amends section 2511(2)(f) of Title 18 to ensure that nothing in chapter 119 or chapter 121 of Title 18 as amended by H.R. 4952, affects existing legal authority for United States Government foreign intelligence activities involving foreign electronic communications systems. The provision neither enhances nor diminishes existing authority for such activities; it simply preserves the status quo. It does not provide authority for the conduct of any intelligence activity.

Further the Committee expects that the practice of providing to the House and Senate Intelligence Committees proposed changes in relevant executive branch procedures and regulations governing the conduct of intelligence activities, including those involving electronic surveillance, physical searches, and the minimization of information collected concerning U.S. persons will be continued. As in the past, the Committee expects that any relevant changes in these procedures and regulations will be provided to the intelligence committees prior to their taking effect.

Finally, as has been noted before, since Congress last addressed the issue of privacy of communications in a comprehensive fashion, the technologies of communication and interception have changed dramatically, and are expected to continue to do so. These factors have raised serious issues about the protection of the privacy interests of U.S. citizens, which are of great concern to this Committee and to the American people. For this reason, the Committee wishes to emphasize the obligation of the heads of intelligence agencies to

continue to keep the Permanent Select Committee on Intelligence fully and currently informed of all intelligence activities pursuant to Title V of the National Security Act of 1947.

Section 107 of H.R. 4952 emphasizes that nothing in Title I of the bill or the amendments made by Title I, such as the changes made to 18 U.S.C. 2511(2)(f), provides authority for the conduct of any intelligence activity.

Subsection (b)(4) of section 101 of the bill amends section 2511(2) to provide new exemptions from criminal liability which are appropriate to the new types of technologies which are added to the privacy protection of the federal wiretap law. Thus, the bill lists a series of types of interceptions which are permissible.

The Committee has drafted the present Act with an eye to its interplay with Section 705(a) of the Communications Act of 1934. In particular, where this bill provides that "it shall not be unlawful" for the public to engage in specific conduct with respect to radio transmissions, the Committee intends that such a provision does not "authorize" the conduct for purposes of the first sentence of Section 705(a) of the Communications Act. Accordingly, the legality of such conduct remains subject to inquiry under the Communications Act. In contrast, where the bill provides that a specified person "may" engage in certain conduct, or uses similar language in the affirmative, the Committee intends that such a provision does "authorize" the conduct for purposes of Section 705(a). The legality of such conduct would be determined under Title 18. In addition, where judicial interpretations have previously determined that certain types of activities are implicitly authorized for purposes of Section 705, that interpretation is intended to continue in effect. *See, e.g., United States* v. *Freeman*, 524 F.2d 337, 340 (7th Cir. 1975), *cert. denied*, 424 U.S. 920 (1976).

The first exemption is a generic exception. It is permissible to intercept electronic communications made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public. The term "configure" is intended to establish an objective standard of design configuration to begin determining whether a system receives privacy protection. An example of systems which are readily accessible include loud speakers hooked up to a telephone system.

It should be noted that the term "readily accessible to the general public" is a defined term with respect to radio communications. See discussion, at ——, *supra*. Under section 101(b)(4) nothing carried by wire is "readily accessible to the general public".

Nothing in the bill affects the use of radar detectors, because the radar transmissions are readily accessible to the general public. Nothing in the bill, however, affects the authority of states to regulate the use of radar detectors.

The second set of exceptions relate to specific types of radio communications which have traditionally been free from prohibitions on mere interception. Thus, it is permissible to intercept any radio communication which is transmitted (1) by any station for the use

of the general public,[86] or that relate to ships, aircraft, vehicles or persons in distress; (2) by any governmental, law enforcement, civil defense, or public safety communications system, including police and fire, readily accessible to the general public; (3) by a station operating on a frequency assigned to amateur, citizens band or general mobile radio services, or (4) by any marine or aeronautical communications system.

Amateur radio communications, including those utilizing telephone interconnect or amateur radio computer linked message systems, are certainly not those to which this legislation is aimed. *All* amateur radio communications conducted on radio frequencies allocated to the Amateur Radio Service are exempt from the electronic communications intercept prohibitions of the bill.

It should be noted that amateurs, in performing their public service functions, occasionally utilize communications of other services, such as NOAA weather broadcasts and the like. As such, many amateurs employ "scanner" receivers which are capable of receiving communications of many different radio services (including amateur VHF and UHF communications, typically). The use of, as an example, a multiband radio receiver by a licensed amateur should not subject the amateur to criminal prosecution or harassment in any fashion. Amateurs have legitimate reason to monitor frequencies outside the amateur bands. Many amateurs, for instance, are enrolled in the Military Affiliate Radio System and the Civil Air Patrol, which use frequencies assigned to the Department of Defense. Others are members of the Coast Guard Auxiliary using frequencies in the Maritime Service allocation. Some 30,000 amateurs are part of Skywarn, a system operated by the National Weather Service for tracking and warning of severe weather conditions, e.g., tornadoes; at times it may be required that they monitor Government frequencies in connection with this work. In short, there is legitimate reason for amateurs to have equipment which tunes beyond amateur bands.

The Committee considered listing all the existing radio services which are exempt from the bar on interceptions, but rejected that approach because it would have been cumbersome, possibly redundant, and would have had a built-in obsolescence. When the Committee asked the Federal Communications Commission for a list of radio services which were currently regulated by the FCC of the same kind as those listed in the bill. they provided a list of more than 40 such services. Such a list is extremely lengthy and the nomenclature used is frequently changing. Therefore, instead of listing all of these services the Committee listed some of the more common radio services. In addition, the bill includes a "generic" exception relating to radio services which are "readily accessible to the general public." Thus, for example, private land mobile services (currently licensed under Part 90 of the FCC Rules) are exempt from the prohibition on interceptions.

This subsection also exempts from coverage any conduct which is also prohibited by section 633 of the Communications Act of 1934.

---

[86] These include all communications transmitted for the use of the general public, including radio and television broadcast signals transmitted under Part 73 of the FCC Rules.

Thus, if an individual violates the criminal prohibitions in section 633 (relating to cable piracy) they cannot also be charged under this chapter of title 18.

The subsection also exempts conduct which is excepted from section 705(a) of the Communications Act by virtue of section 705(b) of that Act. Thus, if conduct is permitted under section 705(b) it would not be a crime under this chapter of title 18. Determination of whether conduct is permitted under section 705(b) must, of course, be the result of an examination of the statute, relevant legislative history, existing court interpretations, and constructions given the statute by appropriate federal regulatory entities.

With respect to the interception of radio communications by home satellite dishes, the Committee does not intend to make criminal any type of conduct that is currently lawful under Section 705 of the Communications Act and the present Wiretap Act. To remove any doubts about its impact on home satellite dish owners, H.R. 4952 contains a provision expressly stating that it is not unlawful under Title 18 to intercept unscrambled network programming feeds to affiliates—*i.e.*, communications "transmitted to a broadcasting station for purposes of retransmission to the general public"—unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain. Accordingly H.R. 4952 does not create a new class of criminal conduct concerning interception of radio communications by home satellite dishes. In order to violate Title 18, moreover, an interception must be "willful". Incidental or inadvertent interception of a protected video signal which does not benefit a home dish owner would not constitute a criminal violation of the statute. H.R. 4952, in short, is carefully drafted to remain as neutral as possible with respect to the coverage of both Section 705 and Title 18 as to interception of radio signals by home satellite dish owners. "Private gain" is a term defined in section 705(b) and the meaning given there is intended to apply to this section as well.

H.R. 4952 adds a new Section 2511(4)(c) which exempts from Title 18 the reception by home earth station owners of certain unscrambled satellite transmissions, as long as such reception is not for commercial advantage or private gain (including any use by a commercial establishment). While the bill does not make criminal any type of conduct with respect to interception of radio communications by home satellite dishes that is currently lawful under section 705 of the Communications Act and the provisions of Chapter 119 of Title 18, the specific exemption in this subsection does not apply to the interception of private communications via satellite such as sporting events when they are not the final output of a national television network to a broadcasting station for purposes of retransmission to the general public.

However, even the unscrambled satellite transmission which is not protected under Title 18 because it comes within Section 2511(4)(b)(iii) may in fact be a private communication, and H.R. 4952 is not intended to exempt such noncommercial interception from liability, if any, under Section 705 of Title 47 or otherwise "authorize" interception of unscrambled transmissions for noncommercial purposes. Rather, the intention of the Committee is that the legality of noncommercial interception of this type of unscrambled satellite transmission will be decided under Section 705 of the Communications Act. The Committee expresses no view on this issue. The Committee notes, however, that it is the view of the General Counsel of the FCC that interception and viewing by home earth station owners of television network satellite feeds to local affiliated television stations could subject the interceptor to civil and criminal penalties under the Communications Act. *See,* Letter of Jack D. Smith to Honorable Robert Kastenmeier, Chairman, Subcommittee on Courts, Civil Liberties and the Administration of Justice, November 27, 1985. *Compare National Football League* v. *McBee & Benno's,* — F.2d— (8th Cir. June 4, 1986) (individual interception of "clean feeds" not permanently enjoined because of equitable considerations).

[The letter follows:]

FEDERAL COMMUNICATIONS COMMISSION,
Washington, DC, November 27, 1985.

Hon. ROBERT W. KASTENMEIER,
Chairman, Subcommittee on Courts, Civil Liberties, and the Administration of Justice, Washington, DC.

DEAR CONGRESSMAN KASTENMEIER: At a recent meeting between congressional and Commission staff, David Beier requested that my office issue an opinion on the applicability of Section 705 of the Communications Act to network television feeds. Specifically, we were asked whether Section 705 prohibits owners of satellite antennas from intercepting the networks' television feeds as they are being distributed to their affiliates via satellite. In general, those transmissions contain network programming and the national commercial spots. Local adveretising and programming are added at the affiliates' broadcast station. Thus, by intercepting the networks' satellite feeds, viewers are seeing essentially the same programs as other television viewers but without certain commercials.

Section 705 provides, in pertinent part that

> No person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by radio and use such communication (or any information therein contained) for his own benefit or for the benefit of another not entitled thereto. . . . This section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication which is transmitted by any station for the use of the general public.

The courts, in several civil and criminal actions, have been the primary interpreters of Section 705. Unfortunately, none of the decided cases are directly on point in that they do not apply to the interception of satellite network feeds. However, the case law applying Section 705 to MDS transmissions strongly suggests that Section 705(a) prohibits the unauthorized interception of satellite network feeds.

The networks' satellite feeds clearly constitute interstate radio communications. Viewing those transmissions constitutes a use by the owner of the satellite antenna of the signal "for his own benefit". *See e.g., Movie Systems, Inc.* v. *Heller,* 710 F. 2d 492 (8th Cir. 1983); *Hoosier Home Theater, Inc.* v. *Adkins,* 595 F. Supp. 889 (S.D.

Ind. 1984). The networks and their local affiliates fund their operations from advertising revenues, which, in turn, are a function of the size of the viewing audience. Because some local commercials are not carried on the network feeds, owners of satellite antennas would not see those commercials and hence would not generally be counted as part of the viewing audience. Therefore, unauthorized interception of the satellite network feeds has the effect of reducing the networks' audience and, as a consequence, their affiliates' operating revenues. In economic terms, this appears to be analogous to the unauthorized interception of subscription television signals without payment.

Section 705(a) expressly excludes from its prohibition radio communications transmitted for the use of the general public. Satellite transmissions, like MDS transmissions, are, however, a common carrier service provided on common carrier frequencies. *See Movie Systems, Inc.* v. *Heller, supra* at 495; *Home Box Office, Inc.* v. *Advanced Consumer Technology, Movie Antenna, Inc.*, 549 F. Supp. 14, 24 (S.D.N.Y. 1981); *Chartwell Communications Group* v. *Westbrook*, 637 F.2d 459, 465 (6th Cir. 1980). For the reason discussed above concerning advertising revenues, they are not intended to be viewed by the general public in the form they are transmitted from satellites. Additionally, in determining the applicability of this exclusion, the critical factor is the intent of the party transmitting the radio communications. *See Chartwell Communications Group* v. *Westbrook, supra* at 464-465. The networks are of course the ultimate authority on their intent. It appears that network satellite feeds are only intended for reception by their affiliates. We believe that the networks are considering scrambling these transmissions in order to preclude their interception. Existing case precedent does not require, however, that networks scramble their signals in order to be encompassed within Section 705. *See Home Box Office, Inc.* v. *Advanced Consumer Technology, Movie Antenna, Inc., supra* at 21-22; *Hoosier Home Theater, Inc.* v. *Adkins, supra* at 396.

Finally, we recognize that under certain conditions, Section 705(b) further excepts from the prohibition of 705(a) the interception of satellite cable programming for private viewing. The satellite network feeds are not, however, satellite cable programming as that term is defined in Section 705(c)(1). Thus, Section 705(b) does not otherwise sanction the interception.

In summation, Section 705(a) appears to encompass the network satellite feeds. Unauthorized interception of those signals by home owners with satellite antennas or the unauthorized sale of decoders could lead to civil or criminal actions under Section 705. *See e.g., Movie Systems, Inc. v. Heller, supra; United States v. Westbrook*, 502 F. Supp. 588 (E.D. Mich. 1980).

Sincerely yours,

JACK D. SMITH, *General Counsel.*

Subsection (g)(iv) also exempts from the criminal prohibitions the interception of any electronic communication the transmission of which is causing harmful interference to any lawfully operating station, to the extent necessary to identify the source of such interference. This exemption was suggested by the Association of North

American Radio Clubs (ANARC) and meets the needs of the Federal Communications Commission.

Finally, this subsection, (g)(v), exempts the interception of a radio communication which is made for other users of the same frequency when such communication is made through a common carrier system that utilizes frequencies monitored by individuals engaged in the provision or use of such a system, as long as the communication is not scrambled or encrypted. This exception will permit the monitoring of shared channels on marine radio which utilizes an onshore operator.

Subsection (b)(4) also amends section 2511(2) to add a new subsection (h). Proposed subsection (h)(i) clarifies that this chapter does not regulate the use of pen registers. The new subsection (h)(ii) states that no violation of this chapter occurs if a provider of wire or electronic communication service records the fact that a communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication or user of that service, from fraudulent, unlawful or abusive use of such a service. This provision permits the electronic and wire communication providers to protect themselves and their customers. Thus, the Committee continues the current law and practice with respect to activities of telephone companies to protect themselves against fraud, abuse or unlawful use. *See United States* v. *Auler*, 539 F.2d 642 (7th Cir. 1976), *cert. denied*, 429 U.S. 1104 (1977); *United States* v. *Goldstein*, 532 F.2d 1305 (9th Cir.), *cert. denied sub nom. Roberts* v. *United States*, 429 U.S. 960 (1976); *United States* v. *Freeman*, 524 F.2d 337 (7th Cir. 1975), *cert. denied*, 424 U.S. 920 (1976); *United States* v. *Clegg*, 509 F.2d 605 (5th Cir. 1975); *United States* v. *Shah*, 371 F. Supp. 1170 (W.D.Pa. 1974).

Proposed subsection (h)(iii) states that it is not unlawful to use a "trap and trace" device. *See Michigan Bell Tel. Co.* v. *United States*, 585 F.2d 385 (6th Cir. 1977) (upholding the use of trap and trace devices under Federal Rule of Criminal Procedure. Rule 41)

Subsection (c) provides technical and conforming amendments. Subsection (c)(1) adds "electronic communication" in appropriate places throughout the chapter.[87] Subsection (c)(2) amends the heading of the chapter. Subsection (c)(3) amends the table of chapters to add electronic communications to the table. Subsection (c) (4), (5), (6) and (7) makes appropriate technical amendments to delete the term "common carrier" and substitute in its place "provider of wire or electronic communication service."

Section 2511(2)(a)(i), as amended, specifies that it is not unlawful for the employees of providers of wire or electronic communication services to intercept customer communications in the normal course of employment while engaged in any activity which is a nec-

[87] Similarly it should be noted that the amendments to section 2511(2)(d) (relating to one—party consent) also apply to private microwave services. It is the Committee's intent to extend the exemption with respect to one—party consent in section 2511(2)(d) to electronic communications. For example, if a licensee of a private microwave system, licensed pursuant to Part 94 of the Federal Communications Commission's Rules, or the operator of a private wireline or private fiber optic system secures consent for the licensee's or operator's recording and/or monitoring of communications over that private system from one of the parties to the communications, such recording and/or monitoring is permissible.

essary incident to the rendition of the service or to the protection of the rights or property of the providor, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality checks. In applying the second clause only to wire communications, this provision reflects an important technical distinction between electronic communications and traditional voice telephone service. The provider of electronic communications services may have to monitor a stream of transmissions in order properly to route, terminate, and otherwise manage the individual messages it contains. These monitoring functions, which may be necessary to the provision of an electronic communication service, do not involve humans listening in on voice conversations. Accordingly, they are not prohibited. In contrast, the traditional limits on service "observing" and random "monitoring" do refer to human aural interception and are retained with respect to voice ("wire") communications.

Subsection (d) modifies the general penalty structure for criminal violations of this chapter. The general rule is that a willful violation is punishable as a five year felony. Thus, unless one of the exceptions applies to a person found guilty of willfully violating one of the criminal statutes in the chapter, they will be liable for a fine under the chapter [88] and imprisonment of up to five years or both.

The first exception for this general rule is that the interception of radio communications are punishable as one year misdemeanors, with fines of up to $100,000 18 U.S.C. 3623. There are three exceptions to this general rule. If the offender has been previously found to have been guilty of an offense of intercepting radio communications, then the felony provisions apply. Similarly, if the interception is done for illegal, tortious or commercial gain purposes, then the offender is punishable under the felony penalty. The second exception is that first offenders who intercept the radio portion of a cellular telephone call (and who act without one of the enumerated bad purposes) may only be subject to punishment of up to six months in prison or a $500 fine or both.

In the event that an offender intercepts the wire portion of a telephone call such conduct remains a five year felony.

The third exception is that conduct, otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted to a broadcasting station for purposes of retransmission to the general public, is not an offense under this chapter and is not subject to civil liability, unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain. The terms "direct or indirect commercial advantage or private financial gain" are intended to have the same meaning as those terms have when used in 47 U.S.C. 705(b). This third exception decriminalizes the interception of "network feeds" under title 18. The exception does not extend beyond "network feeds." The

[88] 18 U.S.C. 3623 provides for a different maximum fine level for felonies, or misdemeanors resulting in death. Individual defendants can be fined up to $250,000 and organizations up to $500,000.

Committee notes that interception and disclosure or use may violate section 705 of the Communications Act. *See* note 9, *supra*.

The penalty structure assumes that more active participation is necessary when a person engages in traditional wiretapping or bugging; therefore, a higher degree of culpability attaches to such conduct. Similarly, higher penalties are justified for second or subsequent offenders or for offenders who engage in prohibited conduct for improper purposes. On the other hand the Committee recognized that although the criminal provisions of the chapter require "willful violations", interception of radio transmissions can be more easily achieved. Therefore, the Committee reduced the penalties for the interception of radio transmissions.

Subsection (e) amends section 2518(10) to provide that the remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions available for non-constitutional violations of this chapter involving such communciations. In the event that there is a violation of law of a constitutional magnitude the court involved in a subsequent criminal trial will apply the existing constitutional law with respect to the exclusionary rule. *Mapp* v. *Ohio*, 367 U.S. 643, 652 (1961); *Massachusetts* v. *Shepperd*, 104 S.Ct. 3424 (1984); *United States* v. *Leon*, 104 S.Ct. 3405 (1984).

Section 102 amends section 2511 of title 18 to add a new criminal prohibition on disclosure by adding a new subsection (3)(A). The new language provides that a person or entity providing wire or electronic communication service to the public shall not willfully divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or the agent of such addressee or intended recipient. The amendment to section 2511 made by § 102 includes the term "to the public" and hereby includes the government as part of the public. Thus, FTS services are included. The term "willfully" is used so as to conform this criminal prohibition with those in the rest of the chapter.

The term "willful" as used in this chapter has been construed—and misconstrued—by the courts. Note, An Analysis of the Term Willfull in Federal Criminal Statutes, 51 NOTRE DAME LAWYER 786 (1976). By retaining the same terminology the Committee does not intend to perpetuate the confusion which has emerged in the case law. See C. Fishman, *Wiretapping and Eavesdropping*, Cum. Suppl. 1985 section 7.15 pages 37–41. Thus, the Committee intends that the term have the same meaning as the term intentional. An "intentional" state of mind means that one's state of mind is intentional as to one's conduct or the result of one's conduct if such conduct or result is one's conscious objective. The intentional state of mind is applicable only to conduct and results. Since one has no control over the existence of circumstances, one cannot "intend" circumstances.

The term "intentional" is narrower than the dictionary definition of "intentional". "Intentional" means more than that one *voluntarily* engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective.

In contrast a knowing state of mind is (1) an awareness of the nature of the conduct, (2) an awareness of or a firm belief in the existence of the circumstance and (3) an awareness of or a firm belief in the substantial certainty of the result.

Thus, the distinction between an "intentional" state of mind and a "knowing" state of mind is narrow but important. As recently stated by Mr. Justice Rehnquist,

> Perhaps the most significant, and most esoteric, distinction drawn by [Model Penal Code] analysis is that between the mental states of "purpose" and "knowledge". As we pointed out in *United States* v. *United States Gypsum Co.*, 438 U.S. 422, 445 (1978), a person who causes a particular result is said to act purposefully (intentionally) "when he consciously desires that result, whatever the likelihood of that result happening from his conduct"; while he is said to act knowingly if he is aware "that the result is practically certain to follow from his conduct, whatever his desire may be as to that result." [footnote omitted.]
>
> In the case of most crimes, "the limited distinction between knowledge and purpose has not been considered important since 'there is good reason for imposing liability whether the defendant desired or merely knew of the practical certainty of the results,'" [citation omitted] * * *

In certain narrow classes of crimes, however, heightened culpability has been thought to merit special attention. *United States* v. *Bailey*, 444 U.S. 394 (1980).

The term "intentional" does not require that the act was committed for a particular purpose or motive. *See* Senate Report 97-307 at 67.

By the use of the term "willful" (throughout chapter 119)—and its accompanying definition—the Committee precludes the applicatin of civil or criminal liability for acts of inadvertent interception.

This section contains an exception to the limitations of divulgence. The exception applies to persons or entities providing wire or electronic communication service to the public. Such persons or entities are permitted to divulge the contents of any such communication if: (1) otherwise authorized in section 2511(2)(A) or 2517 of title 18; (2) with the consent of the originator of any addressee or intended recipient of such communication; (3) to any person employed or authorized, or whose facilities are used, to forward such communication to its destination, or (4) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime if such divulgence is made to a law enforcement agency.

The exceptions to the divulgence bar are relatively straightforward. Obviously providers should be permitted to divulge under other provisions of the chapter. To be consistent with the one party consent exception found in the chapter a similar exception is appropriate here. It is also logical to provide an exception with respect to activities necessary and intrinsic to the communication activity, therefore it is necessary to exempt communication intermediaries. Finally, if a communication provider inadvertently obtains

the contents of a communication during transmission which appears to relate to the commission of a crime, divulgence is permitted when such divulgence is made to a law enforcement agency. If the provider purposefully sets out to monitor conversations to ascertain whether criminal activity has occurred this exception would not apply.

Section 103 amends—largely by recodifying—the existing section 2520 of title 18 to incorporate violations involving interception, disclosure or willful [89] use of wire, oral or electronic communications. Proposed subsection (a) authorizes the commencement of a civil suit. The plaintiff may bring a civil action under Section 2520 whether or not the defendant has been subject to a criminal prosecution for the acts complained of; but in the absence of such prosecution and conviction, it is the plaintiff's burden to establish that the requirements of this section are met. Subsection (b) indicates that appropriate relief can include: (1) preliminary and other equitable or declaratory relief as may be appropriate; (2) damages and punitive damages; and (3) reasonable attorney's fees and other litigation costs reasonably incurred. Subsection (d) of proposed section 2520 provides a method for the computation of damages. Under subsection (c) the court may assess damages consisting of whichever is greater of the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation or statutory damages of whichever is greater of $100 a day for each day of violation or $10,000.

Subsection (d) provides a good faith defense to actions brought under this section. The term "good faith" as used in this section includes the receipt of a facially valid court order. Thus, the fact that the provider of electronic communication service also has received such a court order, means the provider would be entitled to a dismissal of a civil course of action upon a showing that such provider acted within the scope of the court order.

Subsection (e) of proposed section 2520 provides a statute of limitations for actions brought under this section. The subsection provides that any action may not be commenced later than two years after the date upon which the claimant first has reasonable opportunity to discover the violation.

Section 104 amends the list of federal officials who may make applications for court orders under this chapter. Section 2516(1) is amended to add to the list of officials who may be specifically designated by the Attorey General to authorize applications to include any acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division. The addition of an acting Assistant Attorney General is not meant to imply rejection in any other context of the well-established principle that an acting official ordinarily possesses all the legal powers of the official for whom he is acting, *see Keyser v. Hitz*, 133 H.S. 138 (1890), but rather to clarify the law under this statute in light of its unique history and interpretation. *Compare, e.g., United States v. Acon*, 513

[89] The term "willful" is intended to have the same meaning as it does when used in other sections of this chapter.

F.2d 513 (3d Cir. 1975), with *United States v. Pellieci,* 504 F.2d 1106 (1st Cir. 1974), *cert. denied,* 413 U.S. 1122.

Section 105 amends section 2516(1) by adding new crimes which can be used to justify an application for wiretapping or bugging order. The new crimes include violation of the following title 18 provisions: (1) section 751 (relating to escape); (2) sections 2312 and 2313 (relating to automobile theft); (3) the second section 2320 (relating to trafficking in certain motor vehicles or motor vehicle parts); (4) section 1203 (relating to fraud and related activities in connection with access devices); (5) felony violations of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain interception devices); (6) section 3146 (relating to penalty for failure to appear); (7) section 3521 (relating to violations of the security of protecting witnesses); (8) section 32 (relating to destruction of aircraft or aircraft facilities); (9) section 1952A (relating to use of interstate commerce facilities in the commission of murder for hire); (10) section 1952B (relating to violent crimes in aid of racketeering activity); (11) section 115 (relating to threats against a federal official); (12) the section in chapter 65 relating to destruction of an energy facility; (13) section 1341 (relating to mail fraud); and (14) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain intercepting devices). In addition, this section authorizes the application for orders under this chapter for the location of a fugitive from an offense described in this section.

Section 105(b) amends section 2516 to authorize the government to apply for a court order authorizing or approving the interception of an electronic communication by an investigative or law enforcement officer when an interception may provide evidence of a federal felony. Thus, for non-wire, non-oral electronic communications, a different and less restrictive list of crimes can be used to justify an application for interception. Section 105(b) permits the government to make applications for the interception of electronic communications. The Committee has been informed by the Department of Justice that for the three years which follow the date of enactment of this legislation that this exercise of authority will only be made pursuant to the approval of the same level of officials as those involved in the approval of applications for wire intercepts. In addition to this voluntary regulatory limitation, the Department of Justice has committed themselves to submit to the relevant Congressional committees any proposed changes in these regulations at least 90 days in advance of any change.

Section 106 contains four subsections. Subsection (a) provides that a court can authorize an order within the court's jurisdiction and outside that jurisdiction but within the United States in the case of a mobile interception device authorized within such jurisdiction. In the usual case the court will authorize the installation of a device, the device will be installed within the court's jurisdiction and the suspect will then move outside the court's jurisdiction. Nothing in this section affects the current law with respect to the use of such devices outside the United States. In certain cases a device authorized for installation, for instance, in an automobile may be authorized in one district and the vehicle might be moved to another district prior to installation. The authorization will

permit installation in the district to which the vehicle has been moved.

Subsection (b) amends section 2518(4) by striking out "at reasonable rates" and inserting in lieu thereof "for reasonable expenses incurred in providing such facilities or assistance." This is designed to permit reimbursement to be available at an appropriate amount in light of the work required for a particular activity. While in the ordinary case a flat or general rate may be appropriate, this change will permit flexibility to permit reimbursement at a higher level in unusual cases.

Subsection (c) makes two changes in section 2518(5) of title 18. Subparagraph (1) provides a rule for when the 30 days to install a tap or bug begins to run. Under this rule the 30 day time period commences on the earlier of the day on which the officer first begins to conduct an interception or ten days after the order is entered. Under this rule if an officer took 9 days after the entry of the order to effectuate the tap and began to overhear conversations then the 30 day time period would start from on the 9th day.

Subparagraph (2) of subsection (c) of section 106 of the bill provides a special minimization rule. Under this rule when an intercepted communication is in a code or foreign language and an expert in that foreign language or code is not reasonably available during that interception period, minimization may be accomplished as soon as practicable after the interception. In this regard, it is contemplated that the translator or decoder will listen to the tapes of an interception and make available to the investigators the minimized portions preserving the rest for later possible court perusal.

Subparagraph (2) of subsection (c) of section 106 of the bill also provides that the monitoring of interceptions under this chapter may be conducted in whole or in part by Government personnel, or by individuals operating under contract with the Government, as long as such personnel are acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception. This change, which was sought by the Federal Bureau of Investigation, is designed to free field agents from the relatively routine activity of monitoring interceptions so that they can engage in other law enforcement activities.

Subsection (d) of section 106 amends 2518 of title 18 to provide new rules with respect to the specificity required in the descriptions of the place to be bugged or tapped. Under current law, the application and the order must indicate the "particular" facility or place in which the interception is to occur. The amendments establish two largely similar rules, the specificity with which the locale of an interception of "oral communications" and "wire communications" can occur.

With respect to "oral communications" a limited list of federal officials can apply for a special order seeking relief under this provision. The application must contain a full and complete statement as to why the ordinary specification requirements are not practical. The application must also identify the person committing the offense and whose communications are being intercepted. The judge in turn must find that the ordinary specification rules are not practical. Examples of situations where ordinary specification rules

would not be practical would be a suspect who moves from room to room in a hotel to avoid a bug and who sets up a meeting with another suspect for a beach or field. In that case, the order could indicate authority to follow the suspect and engage in the interception once the targeted conversation occurs.

The rule with respect to "wire communications" is somewhat similar. An application for relief from the ordinary specificity rules must be made by a limited list of federal officials. The application must show that the person committing the offense has a purpose to thwart interception by changing facilities. In these cases, the court must find that the applicant has shown that such a purpose has been evidenced by the suspect. An example of a situation which would meet this test would be an alleged terrorist who went from phone booth to phone booth numerous times to avoid interception. Alternatively, a person whose telephone calls were intercepted who said that they were planning on moving from phone to phone or to a pay phone, to avoid detection would have demonstrated that purpose.

Both with respect to "wire" and "dral" communications, where the federal government has been successful in obtaining this relaxed specificity order the government cannot commence the interception until the facilities or place from which the communication is to be commenced is ascertained by the person implementing the interception order. In other words the actual interception could not commence until the suspect commences or evidences an intention to commence a conversation. Thus, it would be improper to use this expanded specificity order to tap a series of telephones, intercept all conversation over such phones and then minimize the conversations collected as a result. This provision puts the burden on the investigatory agency to ascertain when the interception to take place.

Section 107 subsection (a) provides that "* * * (n)othing in this Act or the amendments made by this Act constitutes authority for the conduct of any intelligence activity. This provision clarifies that the amendments made in section 102(b)(3) are not read as constituting any new authority; rather those amendments represent an exemption from this chapter and chapter 121 for otherwise lawful activities.

Section 107(b)(1) exempts communications security monitoring from coverage by Chapter 119 or 121 of Title 18, United States Code. Communications security measures are protective measures taken to deny unauthorized persons information derived from United States Government telecommunications and to ensure the authenticity of such communications. Communications security protection results from the application of security measures to electrical systems generating, handling, processing, or using information the loss of which could adversely affect the national interest. Communications security monitoring is the systematic examination of telecommunications carried out to determine the adequacy of communications security deficiencies, to provide data from which to predict the effectiveness of proposed communications security measures, and to confirm the adequacy of such measures after implementation. Communications security monitoring is an essential part of such examinations and is conducted pursuant to detailed

guidelines approved by the Attorney General. *Supra*, note 11. These procedures generally set forth an elaborate procedure to assure the communications security monitoring of private communications (as defined in para. 4.e.) is based on consent. *See* para. 5.b. and 6.e. of NASCI, 4000A. Communications security monitoring is the act of listening to, copying, or recording transmissions of the Executive Branch official telecommunications, including the communications of certain contractors, to provide technical material for analysis in order to determine the degree of security being provided to these transmissions. This security, includes, for example, that provided by cryptographic equipment. For purposes of communications security monitoring, government telecommunications are telecommunications of any employee, officer, contractor, or other entity of the United States Government which concern an official purpose of government and which are transmitted over a telecommunications system owned or leased by the United States Government or a Government contractor.

Subsection (b) of section 107 provides that this Act does not affect the conduct by officers and employees of the United States Government when such conduct is in accordance with other applicable federal law and if conducted in accordance with procedures approved by the Attorney General. *See e.g.*, Letter from William French Smith, Attorney General, to Lincoln D. Faurer, Director, National Security Agency, dated January 9, 1984 (relating to Guidelines For the Conduct of Communications Security Monitoring Activities, NACSI No. 4000A). The type of activity referred to in this proviso relates to one or more of three categories of activities: (1) interception of encrypted or scrambled or other official communications for communications security of United States Executive Branch department or entities or United States government contractors [90]; (2) interception of radio communications transmitted between or among foreign powers or agents of foreign powers; or (3) accessing electronic communication systems used exclusively by a foreign power or an agent of a foreign power.

[The letter follows:]

OFFICE OF THE ATTORNEY GENERAL,
Washington, DC., January 9, 1984.

LINCOLN D. FAURER,
Lieutenant General, USAF,
Director, National Security Agency,
Ft. George G. Meade, MD.

DEAR DIRECTOR FAURER: The attached procedures governing the communications security (COMSEC) activities of the United States government meet the requirements of Executive Order 12333 and are otherwise lawful. Accordingly, they are hereby approved.

[90] Government contractor means an individual, corporation, partnership or other entity performing work under a United States Government contract.

[Paragraph regarding internal policy discussions unrelated to lawfulness of the procedures deleted.]

Sincerely,

WILLIAM FRENCH SMITH,
Attorney General.

Attachments.

NACSI NO. 4000

GUIDELINES FOR THE CONDUCT OF COMMUNICATIONS SECURITY MONITORING ACTIVITIES

1. REFERENCES

a. Communications Act of 1934, Public Law 73-416 (as amended).
b. Omnibus Crime Control and Safe Streets Act of 1968, Public Law 90-351 (as amended).
c. Foreign Intelligence Surveillance Act of 1978, Public Law 95-511.
d. National Communications Security Directive, dated 20 June 1979.
e. Executive Order 12333, "United States Intelligence Activities," dated 4 December 1981.

2. INTRODUCTION

The basic purpose of communications security (COMSEC) monitoring is to provide unique material, not readily available through other sources, to evaluate the status of U.S. COMSEC. The information collected through the COMSEC monitoring program is similar to the information potentially available to foreign powers through their own signals intelligence (SIGINT) collection. Hypothetical projections of the vulnerability of telecommunications, procedures, equipment, and systems, based on technical analysis and modeling, do not always provide a comprehensive data base for analysis. COMSEC monitoring is, therefore, used to provide the empirical data necessary to conduct comprehensive analyses of these vulnerabilities and afford a basis for correcting them.

3. PURPOSE AND SCOPE

a. This Instruction provides policy and guidance for the establishment of COMSEC monitoring procedures consistent with applicable law and regulations.* It implements that portion of the National Communications Security Directive (Reference d.) which assigns the Director, National Security Agency (NSA), responsibility to issue guilelines for the conduct of COMSEC monitoring.

b. This Instruction is applicable to all Federal Government departments and agencies engaged in or using the results of COMSEC monitoring. It has been approved by the Attorney General.

* Although there are no Federal statutes specifically addressing COMSEC, References a., b., and c. will have an impact upon any COMSEC monitoring guidelines and procedures.

c. Technical surveillance countermeasures, electronic sweeps, surveillance of non-communications emissions (e.g., radar), and TEMPEST testing are not within the scope of this Instruction.

4. DEFINITIONS

a. *COMSEC.* Protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including cryptosecurity, transmission security, and emissions security) to electrical systems generating, handling, processing, or using national security or national security-related information. It also includes the application of physical security measures to COMSEC information or materials.

b. *COMSEC Monitoring.* The act of listening to, copying, or recording transmissions of one's own official telecommunications to provide material for analysis in order to determine the degree of security being provided to those transmissions.

c. *Contents.* When used with respect to a communication, it includes any information concerning the identity of the parties thereto, or the existence or meaning of that communication.

d. *Electronic Surveillance.* The acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

e. *Private Communication.* A communication in which the parties thereto, in the absence of their consent to be monitored for COMSEC purposes, have a reasonable expectation of privacy.

f. *Telecommunications.* The transmission, communication, or processing of information, including the preparation of such information therefor, by electrical, electromagnetic, electromechanical, or electro-optical means.

g. *Telecommunications System.* The devices used to transmit and/or receive communications or process telecommunications, including the preparation of information, therefor; the devices may be electrical, electromagnetic, electromechanical, or electro-optical.

h. *Government Telecommunications.* Telecommunications of any employee, officer, contractor, or other entity of the U.S. Government which concern an official purpose of Government and which are transmitted over a telecommunications system owned or leased by the U.S. Government or a Government contractor. (See Telecommunications and Telecommunications System, above.)

5. POLICY

a. The Government will conduct COMSEC monitoring activities only as necessary to determine the degree of security provided to Government telecommunications and aid in countering their vulnerability. Such activities shall be conducted in strict compliance with current law, executive orders, and policy.

b. Government telecommunications systems are subject to COMSEC monitoring by duly authorized Government entities. The use of such systems by any person shall be construed to imply con-

sent to the monitoring for COMSEC purposes of communications carried over them.** Users of these systems must be properly notified in advance, in accordance with the guidelines in subparagraph 6.e., below, that their use of these systems constitutes consent to monitoring for COMSEC purposes. The Government shall not monitor telecommunications systems which are owned or leased by Government contractors for their own use without first obtaining the express written approval of the chief executive officer of the contractor organization (or his designee) and the written opinion of the General Counsel of the department or agency which is conducting the monitoring that procedures, such as those contained in subparagraph 6.e., below, have been implemented sufficiently to afford adequate notice to the contractor organization's employees.

c. The Government shall not monitor for COMSEC purposes the contents of any telecommunication when such monitoring would constitute electronic surveillance.

d. In accordance with procedures approved by the Attorney General information acquired incidentally from Government telecommunications during the course of authorized COMSEC monitoring which relates directly to a significant crime will be referred to the military commander or law enforcement agency having appropriate jurisdiction. When taking such action, the General Counsel of the department or agency which is conducting the COMSEC monitoring shall be notified promptly. The results of COMSEC monitoring may not be used in a criminal prosecution without prior consultation with the General Counsel of the department or agency which performed the monitoring.

e. The results of COMSEC monitoring shall not be used to produce foreign intelligence or counterintelligence, as defined in Reference e. However, the results of COMSEC monitoring of U.S. and Allied military exercise communications may be used for exercise intelligence purposes under procedures prescribed in applicable directives.

f. No department or agency may monitor the telecommunications of another department or agency for COMSEC purposes without the express prior written approval of a responsible official of the department or agency to be monitored, except as provided for in subparagraph 8.b.(2).

g. It is recognized that COMSEC monitoring operations conducted in a crowded telecommunications environment may result in the temporary acquisition of private communications. COMSEC monitoring shall be conducted in accordance with operational procedures which minimize the possibility that the contents of such telecommunications will be acquired. Such procedures shall be consistent with the guidelines contained herein and shall be endorsed by the General Counsel of the department or agency issuing the procedures.

** Consent to COMSEC monitoring is required of only one party to a conversation or transmission.

6. GUIDELINES FOR THE CONDUCT OF COMSEC MONITORING

a. COMSEC monitoring may be undertaken for the following reasons appropriate to the purpose described in paragraph 2., above:

(1) To collect operational signals needed to measure the degree of security being achieved by U.S. codes, cryptographic equipment and devices, COMSEC techniques, and related materials.

(2) To provide a basis from which to assess the types and value of information subject to loss through intercept and exploitation of Government telecommunications.

(3) To provide an empirical basis for improving the security of Government telecommunications against SIGINT exploitation.

(4) To assist in determining the effectiveness of Electronic Countermeasures/Electronic Counter-Countermeasures (ECM/ECCM) and cover and deception measures.

(5) To identify Government telecommunication signals that exhibit unique external signal parameters, signal structures, modulation schemes, radio fingerprints, etc., that could provide SIGINT elements of foreign powers the capability to identify specific targets for subsequent geopositioning and exploitation purposes.

(6) To provide empirical data to train users of Government telecommunications systems in proper COMSEC techniques and measures.

(7) To evaluate the effectiveness of COMSEC education and training programs.

(8) To train personnel and to test the capability of COMSEC monitoring equipment.

b. The following categories of telecommunications are not considered private for purposes of this Instruction. Accordingly, acquisition of the contents of any communications in these categories which may occur in the course of locating or examining Government telecommunications is not electronic surveillance.

(1) Commercial broadcast radio communications.

(2) Public safety, citizens band, amateur radio, and similar radio systems licensed by the Government for public use or access.

(3) Any communications in portions of the electromagnetic spectrum which are allocated by the Government for its own use.

c. No incidentally acquired private communication may be monitored beyond the point where a determination can reasonably be made that it is private. A record of the acquisition may be kept for signal identification and avoidance purposes; such a record may describe the signal parameters (frequency, modulation, type, and timing) but may not identify the contents of the communication.

d. Contents of any private communication may not be deliberately acquired as part of a procedure for locating, identifying, or monitoring a Government communication.

e. Notice of the existince of COMSEC monitoring in conformance with subparagraph 5.b., above, can be accomplished by any of the following means or any combination thereof which the legal coun-

sel of the affected department or agency considers legally sufficient to achieve proper notification in terms of content, prominence, and specificity.

(1) Decals placed on the transmitting or receiving devices.

(2) A notice in the daily bulletin or similar medium.

(3) A specific memoradum to users.

(4) A statement on the cover of the official telephone book or communications directory.

(5) A statement in the standing operating procedures, communications-electronics operating instructions, or similar documents.

7. CONTROL OF MONITORING RECORDS AND EQUIPMENT

a. All reports, logs, and material produced in the course of COMSEC monitoring will be afforded protection commensurate with the classification of the information and the sensitivity of the monitored activity. Reports or material produced from COMSEC monitoring which identify security weaknesses of the monitored activity will be classified at least confidential and downgraded to unclassified when security weaknesses are corrected.

b. Interim and final reports may be disseminated only to the extent necessary for COMSEC purposes except as provided for in subparagraph 5.d., above. These reports shall not contain any information extraneous to COMSEC purposes, or names of individuals or sufficient data to identify the source except in an official capacity; e.g., "the radio operator on watch." Dissemination controls should be expressly stated on each report.

c. All COMSEC monitoring recordings and written records, logs, and notes shall be destroyed as soon as operationally feasible.

d. Except as provided for in subparagraph 5.d., above, no information extraneous to COMSEC purposes will be recorded, reported, noted, logged, or filed. If within the capabilities of COMSEC monitoring equipment, any such information that is inadvertently acquired shall be expunged upon recognition. All monitoring records shall be reviewed for identification and expungement of extraneous information within a reasonable time after they are created.

e. Access to and dissemination of COMSEC monitoring recordings or written records, reports, logs, and notes shall be limited to that which is necessary for COMSEC purposes. No access to, or dissemination of, such materials beyond COMSEC operational elements shall be allowed until such material is reviewed to determine that it contains no information extraneous to COMSEC purposes.

f. COMSEC monitoring equipment systems shall be safeguarded to prevent unauthorized access and use.

8. RESPONSIBILITIES

a. Heads of departments and agencies shall:

(1) Provide for and conduct COMSEC monitoring operations as they deem appropriate, subject to the provisions of law, executive orders, policy, and this Instruction.

(2) Develop procedures for the conduct of COMSEC monitoring, consistent with the policy and guidelines herein, in collaboration with the Director, NSA. Such procedures shall be approved by the Attorney General.

b. The Director, NSA shall:

(1) Advise and assist other departments and agencies in establishing their operating procedures to implement this Instruction.

(2) Monitor fielded Government cryptography as necessary to discharge his responsibilities under the National COMSEC Directive, provided that prior notice will be given to the organization whose encrypted telecommunications are to be monitored. No monitoring will be conducted which results in or affords a substantial likelihood that the plaintext of a communication, other than short-duration plaintext operator conversations associated with establishing a secure condition, will be acquired without the prior approval of the entity whose telecommunications are to be monitored.

LINCOLN D. FAURER,
Lieutenant General, USAF, Director.

Section 108 contains three subsections. Subsection (a) amends chapter 205 of title 18 to add a new section 3117. This section provides that if a court is authorized to issue a warrant or other order for the installation of a mobile tracking device, such an order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction. It should be noted that, unlike a mobile interception device, a tracking device may be utilized outside the United States once the device is installed within the court's jurisdiction. Subsection (b) of the proposed section contains a definition. "Tracking device" is defined to mean an electronic or mechanical device which permits the tracking of the movement of a person or subject.

Subsection (b) of section 108 contains a technical amendment to amend the table of chapters.

The provisions of this section are intended to permit the installation of tracking devices which may move from district to district. The section does not affect the legal standard for the issuance of orders authorizing the installation of each device. *See generally United States v. Karo,* 104 S. Ct. 3296 (1984) (a search warrant not required where the owner consents to installation); *United States v. Knotts,* 460 U.S. 276 (1983) (installation of a beeper on a container to follow on a public roadway does not violate the Fourth Amendment). The Court in *Karo, supra,* did find that if investigators used a beeper to determine whether the beepered object is in a private location, a warrant is required. *See Fishman, Electronic Tracking Devices and the Fourth Amendment: Knotts, Karo and the Questions Still Unanswered,* 34 CATH. UNIV. L. REV. 277 (1985).

Section 109 adds two new offenses to section 2232 of title 18. The first new offense is to warn or give notice to a person that they are the subject of an act of interception under title 18. The elements of the offense require that the defendant have knowledge [91] that the federal law enforcement or investigative officer has been authorized or has applied for an interception order. The defendant need

[91] See House Report 96-1396, *Criminal Code Revision Act of 1980,* at 32-36.

not know that such an application was under a particular chapter of federal law, rather, only that such application or order was under federal law. The defendant must engage in conduct of giving notice of the possible interception to the person who was or is the subject of the interception. *See* House Report 96-1396 at 32-36. Finally, the defendant must be shown to have engaged in such conduct with a specific motive such as to obstruct, impede or prevent the interception. Finally, the offense also includes attempts to engage in the offense.

The penalty for a violation of this new offense is a possible prison term of up to five years, a fine under this title, or both.

The second new offense set forth in section 109 is to warn the subject of an act of electronic surveillance under the Foreign Intelligence Surveillance Act (FISA). The elements of the offense are identical except that that type of surveillance order is governed by a different statute (FISA) and that statute authorizes a slightly different type of surveillance activity. The penalties for this offense are the same as the aforementioned offense.

Section 110 provides a new section 2521 in title 18. This new section adds to the existing panoply of criminal and civil remedies by authorizing the Attorney General to obtain an injunction to prevent felony level violations of this chapter. This provision is modelled after a similar statute (injunctions against fraud) enacted by Congress in the Comprehensive Crime Control Act of 1984, Public Law 98-473, *see also* Senate Report 97-307 at 1267. This section directs the court to proceed as soon as practicable to the hearing and determination of the matter. This section also provides that preliminary relief can be granted to prevent injury during the pendency of the action. A proceeding under this section is governed by the Federal Rules of Civil Procedure (particularly Rule 65). In the event, however, that an indictment has been returned against the respondent then discovery by both sides is limited to that permissible under the Federal Rules of Criminal Procedure.

Section 111 provides the effective date for the amendments made by this title. Subsection (a) of this section provides the general rule, that except as provided in subsection (b) the amendments made in this title take effect 90 days after the date of enactment. In the case of conduct pursuant to a court order or extension such amendments only apply with respect to court orders or extensions made after this title takes effect. The exception found in subsection (a) is written to permit the continuation under the old law rules of interceptions authorized under such rules. Because ongoing investigations may involve lengthy interceptions, any new order or extension of an order made after the general effective date will be governed by the new law rules.

Subsection (b) of section 111 provides a special rule for state authorization of interceptions. This special effective date rule is necessary because the provisions of chapter 119 of title 18 supersede previous state laws, to the extent that they exist, with respect to electronic communications. Under the provisions of chapter 119 the various states must enact statutes which are at least as restrictive as the provisions of chapter 119 before they can authorize their state courts to enter such interception orders. Because of the massive number of changes made in chapter 119 by this title in relation to electronic communication, it seemed appropriate to grant the states sufficient time to modify their laws accordingly. The special rule, in essence, gives the states two years to bring their laws into conformity with these amendments of chapter 119 of title 18. It is possible that state laws will not need be changed to accommodate revisions on interceptions of wire or oral communications. Any such changes would also benefit from the two-year delayed effective date.

TITLE II—STORED AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORD ACCESS

Section 201 amends title 18 by adding a new chapter 121 which consists of ten new proposed sections. These sections are discussed below.

Proposed section 2701 provides a new criminal offense. The offense consists of either: (1) intentionally accessing, without authorization, a facility through which an electronic communication service is provided or (2) intentionally exceeding the authorization of such facility. In addition, the offense requires that the offender must, as a result of such conduct, obtain, alter or prevent unauthorized access to a wire or electronic communication while it is in electronic storage in such a system. The term "electronic storage" is defined in section 2510(17) of title 18. Electronic storage means any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof and the storage of such communication by an electronic communication service for purposes of back-up protection of such communication.

Section 2701(a) makes it an offense intentionally to access without authorization, or to exceed an authorization to access, an electronic communication service and thereby obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system. This provision addresses the growing problem of unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public. The Committee recognizes, however, that some electronic communication services offer specific features, sometimes known as computer "electronic bulletin boards," through which interested persons may communicate openly with the public to exchange computer programs in the public domain and other types of information that may be distributed without legal constraint.

It is not the Committee's intent to hinder the development or use of "electronic bulletin boards" or other comparable services. The Committee believes that where communications are readily accessible to the general public, the sender has, for purposes of Section 2701(a), extended an "authorization" to the public to access those communications. A person may reasonably conclude that a communication is readily accessible to the general public if the telephone number of the system and other means of access are widely known, and if a person does not, in the course of gaining access, encounter any warnings, encryptions, password requests, or other indicia of intended privacy. To access a communication on such a system should not be a violation of the law.

Some communication systems offer a mixture of services some, such as bulletin boards, which may be readily accessible to the general public, while others—such as electronic mail—may be intended to be confidential. Such a system typically has two or more distinct levels of security. A user may be able to access electronic bulletin boards and the like merely with a password he assigns to himself, while access to such features as electronic mail ordinarily entails a higher level of security (i.e., the mail must be addressed to the user to be accessible specifically). Section 2701 would apply differently to the different services. Those wire or electronic communications which the service provider attempts to keep confidential would be protected, while the statute would impose no liability for access to features configured to be readily accessible to the general public.

Section 2701(a) generally prohibits any person from intentionally accessing a wire or electronic communication system without authorization or in excess of authorization, and thereby obtaining access to a wire or electronic communication while it is in electronic storage in the system. An "electronic mail" service, which permits a sender to transmit a digital message to the service's facility, where it is held in storage until the addressee requests it, would be subject to Section 2701. A "voice mail" service operates in much the same way, except that the stored message takes the form of the sender's voice, usually in digital code. It would likewise be subject to Section 2701. Similarly, to the extent that a remote computing service is provided through an Electronic Communication Service, then such service is also protected.

A person found guilty of this new offense is subject to a maximum penalty as specified in subsection (b) of proposed section 2701. Subsection (b) provides a general rule that such an offense is punishable by a fine of $5,000 or imprisonment of not more than six months, or both. There are two exceptions to this general rule. If the offender has acted for purposes of commercial advantage, malicious destruction or damage, or private financial gain, the possible penalty is escalated to a fine of up to $250,000 and a prison term of up to one year or both. The second exception is to increase the potential jail term for second or subsequent offenders up to two years in prison.

In light of the importance of communications generally to interstate and foreign commerce, the prevention of unauthorized access to the systems used for such communication is a legitimate federal concern. In some instances, unauthorized access to wire or electronic communications is undertaken for purposes of malice or financial advantage. Other instances, however, arise from the activities of computer amateurs, often called "hackers," whose goal is primarily the access itself. Still, "hacking" cannot be dismissed as a harmless prank; a hacker may stumble across sensitive or commercially useful information, and in any event invades the privacy of those whose communications are stored. It is thus important to prohibit unauthorized access even if undertaken without a malicious purpose or motive. Section 2701(b)(1) does, however, specify higher penalties for unauthorized access committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain.

Subsection (c) of proposed section 2701 provides that this section does not apply with respect to conduct which is authorized by: (1) the provider of the service; (2) the user of the service; or (3) the provisions of sections 2703 or 2704 of this new chapter.

Proposed section 2702 provides general prohibitions on the disclosure of contents. This proposed section provides that a person or entity providing electronic communication services to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service. This prohibition is similar to that found in chapter 119 with respect to the divulgence of a wire or electronic communication during transmission. The term knowingly means that the defendant was aware of the nature of the conduct, aware of or possessing a firm belief in the existence of the requisite circumstances and an awareness of or a firm belief about the substantial certainty of the result. The conduct in question is the act of disclosure. The result is that the contents have been provided to another person or entity. The circumstances involved are that the person involved provides electronic communication services to the public and that the contents relate to a wire or electronic communication. Knowledge as to a circumstance includes willful blindness, *Model Penal Code* section 2.02. Comment at 129–30 (Tent. Draft No. 4, 1955); *United States* v. *Jewell*, 532 F.2d 697 (9th Cir.), *cert. denied*, 426 U.S. 951 (1976). The concept of "knowingly" does not include, however, "reckless" or "negligent" conduct. *See* HOUSE REPORT 96–1396 at 33–34 (for a definition of terms). This provision is aimed at proscribing the disclosure of stored wire and electronic communications. Subsection (b) contains the exceptions to this general rule.

Subsection (a)(2) of proposed section 2702 provides that a person or entity providing remote computing services to the public shall not knowingly divulge the contents of any communication which is carried or maintained on that service if certain conditions are met. The term "contents" as used in section 2702 is intended to encompass the substance, purport, effect or meaning of the communication. Under this interpretation, a service provider is allowed to divulge mailing lists that identify persons fitting broad demographic criteria. Unless otherwise authorized, service providers may not divulge to third parties information that profiles the activities of individual subscribers through the divulgence of the contents of a communication. The first condition is that the affected communication must be on behalf of and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from) a subscriber or customer of such service. The second condition is that the affected communication be solely for the purpose of providing storage or computer processing services to such subscriber or customer, so long as the provider is *not* authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing. The prohibitions of this subsection are also modified by the exceptions in subsection (b).

Section 2702(a) protects communications "received by means of electronic transmission from * * * a subscriber or customer of such service" and kept "solely for the purpose of providing storage or

computer processing services to such subscriber or customer * * *." In the case of either electronic mail or voice mail, the sender—a user of the service—has necessarily authorized the addressee's access to the message. The addressee's acquisition of the message is therefore clearly within the contemplation of section 2701(c). Sometimes the addressee, having requested and received a message, chooses to leave it in storage on the service for re-access at a later time. The Committee intends that, in leaving the message in storage, the addressee should be considered the subscriber or user from whom the system received the communication for storage, and that such communication should continue to be covered by section 2702(a)(2).

Section 2702(a) generally prohibits the provider of a wire or electronic communication service to the public from knowingly divulging the contents of any communication while in electronic storage by that service to any person other than the addressee or intended recipient of such communication, or an agent of such addressee or intended recipient. Similarly, section 2511(3) of title 18, as amended, prohibits such a provider from divulging the contents of a communication while it is in transmission. Neither provision, however, nor any other provision in the Act, is intended to affect any other provision of federal law that prohibits the disclosure of information on the basis of the content of the information, such as the Fair Credit Reporting Act.

The application of sections 2701(a) and 2511(3) is limited to providers of wire or electronic communications services. There are instances, however, in which a person or entity both acts as a provider of such services and also offers other services to the public. In some such situations, the bill may allow disclosure while another federal requirement, applicable to the person or entity in another of its roles, prohibits disclosure. The Committee intends that such instances be analyzed as though the communication services and the other services were provided by distinct entities. Where a combined entity in its non-provider role would not be allowed to disclose, the appropriate outcome would be non-disclosure.

One example of such an instance could arise under the Fair Credit Reporting Act, 15 U.S.C. 1681b, which limits the circumstances under which consumer reporting agencies may disclose certain information relating to consumers. An entity may perform a consumer reporting agency function, and may also provide wire or electronic communication services to the public. Such an entity might provide itself with electronic communication services, including the storage of data relating to consumers. Sections 2701(a) and 2511(3) have no effect on the entity's role as a consumer reporting agency, and in that role the entity must comply with the disclosure limitations of the Fair Credit Reporting Act.

Section 2702(a)(2) prohibits the provider of a remote computing service to the public from knowingly divulging the contents of any communication carried or maintained on the service on behalf of, and received by means of (or created from communications received by means of) electronic transmission from a subscriber or customer of the service, and carried or maintained solely for the purpose of providing such service to the subscriber or customer. This provision reflects the rapidly growing importance of information storage and processing to the Nation's commerce. Today, the subject matter of commerce increasingly is information in electronic form and the processing of information itself has become a major industry. The secure storage of electronic information has thus become as important to the commercial system as the protection of paper records. Accordingly, where an electronic communication is transmitted by a subscriber or customer to such a service, and is stored on the subscriber's behalf solely for the purpose of providing storage or computer processing services to the subscriber, the Committee intends that the communication—together with the products of any processing that the service performs for the customer—remain available only to the subscriber and to the persons he designates, with certain exceptions enumerated in Section 2702(b).

Section 2702 specifies that a person or entity providing wire or electronic communication service to the public may divulge the contents of a communication while in electronic storage by that service with the lawful consent of the originator or any addressee or intended recipient of such communication. The Committee emphasizes that "lawful consent," in this context, need not take the form of a formal written document of consent. A grant of consent electronically would protect the service provider from liability for disclosure under Section 2702. Under various circumstances, consent might be inferred to have arisen from a course of dealing between the service provider and the customer or subscriber—*e.g.*, where a history of transactions between the parties offers a basis for a reasonable understanding that a consent to disclosure attaches to a particular class of communications. Consent may also flow from a user having had a reasonable basis for knowing that disclosure or use may be made with respect to a communication, and having taken action that evidences acquiescence to such disclosure or use—*e.g.*, continued use of such an electronic communication system. Another type of implied consent might be inferred from the very nature of the electronic transaction. For example, a subscriber who places a communication on a computer "electronic bulletin board," with a reasonable basis for knowing that such communications are freely made available to the public, should be considered to have given consent to the disclosure or use of the communication. If conditions governing disclosure or use are spelled out in the rules of an electronic communication service, and those rules are available to users or in contracts for the provision of such services, it would be appropriate to imply consent on the part of a user to disclosures or uses consistent with those rules.

Section 2702(a) specifies that a person or entity providing a wire or electronic communication service or remote computing services to the public shall not knowingly divulge the contents of any communication while in electronic storage by that service to any person or entity other than the addressee or intended recipient of such communication or an agent of such addressee or intended recipient. Under Section 2702(b), disclosure to any other person requires the consent of the originator or any addressee or intended recipient of the communication. Under some circumstances, however, a customer of or subscriber to a wire or electronic communication service may place a communication on the service without specifying an addressee. The Committee intends, in that situation,

that the communication at a minimum be deemed addressed to the service provider for purposes of Section 2702(b). Because an addressee may consent to the disclosure of a communication to any other person, a service provider or system operator, as imputed addressee, may disclose the contents of an unaddressed communication.

A person may be an "intended recipient" of a communication, for purposes of Section 2702, even if he is not individually identified by name or otherwise. A communication may be addressed to the members of a group, for example. In the case of an electronic bulletin board, for instance, a communication might be directed to all members of a previously formed "special interest group" or, alternatively, to all members of the public who are interested in a particular topic of discussion. In such an instance, the service provider would not be liable for disclosure to any person who might reasonably be considered to fall in the class of intended recipients.

Subsection (b) of proposed section 2702 provides six distinct exceptions to the general limitations on divulgence contained in subsection (a). The first exception is with respect to divulgence to an addressee or intended recipient of a communication or an agent thereof. Section 2702(b) which places limits on disclosure. In connection with disclosures made pursuant to section 2702(b)(4), these limitations apply along the agent claim, the second exception is divulgence authorized by statutory provisions in either chapter 119 or this chapter. The third exception is divulgence with the lawful consent of the originator, addressee, or intended recipient (or subscriber in the case of remote computer service). The fourth exception is to permit divulgence to a person who is involved in forwarding the communication to its destination. The fifth exception permits divulgence necessarily incident to the rendition of such services or to the protection of the rights or property of the provider of the services. The terms "rights" and "property" here refer to such rights as intellectual property rights, the right to be free from the theft of services. The term is not intended to be read as to permit a provider to contract with an unauthorized party an obligation to divulge all stored messages, without notice to or any consent from the originator of the message, and then to claim that such divulgence is to protect the rights in such a contract. The sixth exception authorizes the divulgence to a law enforcement agency if the contents of the communication were inadvertently obtained and appear to pertain to the commission of a crime. This exception is intended to be read narrowly. A systematic practice of reviewing stored communications to look for evidence of a crime could not qualify as inadvertent.

Proposed section 2703 contains the procedural requirements for the government to obtain access to electronic communications in storage and transactional records relating thereto. Proposed section 2703 contains four subsections.

Subsection (a) sets forth the requirements which must be met before the government may obtain access to the contents of a non-voice wire communication or an electronic communication in storage. As a general rule the government must obtain a search warrant. The contents of the voice portion of a wire communication in storage such as with "voice mail" may not be obtained under this

section. Under the provisions of chapter 119 of title 18 apply. The general rule applies to electronic communications which have been in electronic storage for 180 days or less. The government is, however, permitted to use alternative means of obtaining access if the communication has been in storage for more than 180 days. For this second category of stored records, the government may use an administrative subpoena authorized by federal or state law or a federal or state grand jury subpoena or a court order under subsection (d) of this section, provided that the customer obtains notice. There is an exception for the notice required for this alternative means, and that exception is set forth in proposed section 2704.

The Committee required the government to obtain a search warrant because it concluded that the contents of a message in storage were protected by the Fourth Amendment. The reasons for such a conclusion are set forth more completely earlier in this report. The Committee recognized that electronically stored communications can be of two types. The first type of stored communications are those associated with transmission and incident thereto. The second type of storage is of a back-up variety. Back up protection preserves the integrity of the electronic communications system and to some extent preserves the property of the users of such a system. Most—if not all—electronic communications systems (such as electronic mail systems), however, only keep copies of messages for a few months. To the extent that the record is kept beyond that point it is closer to a regular business record maintained by a third party and, therefore, deserving of a different standard of protection.

Subsection (b) sets forth the procedures the government must use before it can obtain access to the contents of any electronic communication held by a provider of remote computing services. The government may proceed using any of three alternative means of access. The government may, without providing the required notice to the subscriber or customer, obtain a search warrant. The government may also choose to obtain access by giving notice to the subscriber or customer, and using either (a) an administrative summons authorized by federal or state law or a grand jury subpoena; or (2) a court order under subsection (d). The requirement that the state law authorize the use of a grand jury subpoena or administrative summons for purposes of obtaining access to such records—and the parallel requirement in subsection (d) that a court order be obtained under certain standards—are intended to apply the relevant state law with respect to the legal standard such officials must meet with respect to access to those records. Thus, to the extent that a state law or State Constitution requires that a court order based on a standard other than relevance be obtained by a state government official before such official can obtain access to the type of records protected by this chapter, then that law would preclude the use of the provisions of this section with respect to state government officials. Thus, state laws such as those found in Colorado, California, New Jersey and Pennsylvania would remain unaffected with respect to access by state government officials. *See* discussion of records access, *supra*. To the extent that such access is sought by a federal official under the conditions specified under this section, then state law is overridden by virtue of the Suprema-

cy Clause. Examples of such federal legal authority include administrative summons used by the Drug Enforcement Administration, 21 U.S.C. 876, and by the Internal Revenue Service, 26 U.S.C. 7609. Nothing in this authorization eliminates any notice which may be required under other laws. *See, e.g.,* 26 U.S. 7609. The notice required under subsection (b)(1)(B) (i) and (ii) may be dispensed with if the conditions of section 2704 have been met. The type of records to which the provisions of subsection (b) apply are set forth in subsection (b)(2).

The type of electronic communication held by a remote computing service which is protected from governmental access is limited by certain preconditions. The communication must be on behalf of a subscriber or customer of a remote computing service and such communication must have been given to the remote computer service under narrow conditions. The narrow conditions are that the communication must have been received in a certain form (i.e. by means of electronic transmission or similar means). In addition, the communication must have been surrendered solely for the purpose of providing storage or computer processing services to the subscriber or customer, and the provider may not be authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

Subsection (c) sets forth the rules under which the government may require the provider of electronic communications services or remote computing services to disclose a record or other transactional information concerning a subscriber or customer (other than the contents of a communication). The type of records involved are billing records and telephone toll records (including the record of long distance numbers and message unit detailing information). The government need not provide notice to the subscriber or customer before it seeks access to these types of records. On the other hand, the government must use one of three sets of authorized procedures. The government can rely on administrative subpoenas or grand jury subpoenas to the extent that such processes are legally authorized. Alternatively, the government can use a search warrant. Finally, the government can seek a court order directing the disclosure of such records. If a court order is sought then the government must meet the procedural requirements of subsection (d).

Subsection (d) provides that the government shows that there is reason to believe that the contents of an electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry. The only contents which can be sought using the court order option are, of course, those stored for more than 180 days.

It should be noted that when the government is required to give notice to the customer or subscriber that the purpose of such notice is to provide the subscriber or customer with an opportunity to contest the propriety of such a disclosure. The customer or subscriber has standing to raise any legitimate defense to such disclosure including any constitutional claims under the First, Fourth, Fifth or Fourteenth Amendments, any claims of privilege, and any available defenses to improperly issued subpoenas. Whether any of these claims are accepted by the court before whom the application is pending will depend on the facts of a given case and the state of the law at the time.

Proposed section 2704 sets forth in four subsections the procedures governing back-up copy preservation.

Subsection (a)(1) provides that when the government is seeking access to remote computing service information on records under section 2703(b)(2) that the government can seek and obtain the assistance of the provider in preserving the information or records sought. The government may, under this subsection include with its subpoena or court order a request that the provider create or generate a back-up copy of the requested records or information. The provider is directed to create a back-up copy as soon as practicable consistent with its regular business practices. Thus, if a service promotor maintains back-up copies as part of its regular business activities, it does not have to create a new copy. The provider is directed not to inform the customer or subscriber of this activity. After the copy has been made the provider is directed to inform the governmental entity seeking the copy that it has complied with the request. Finally, this subsection sets as an outside limit for the creation of a back-up copy of two business days.

Subsection (a) provides that once the governmental entity has received confirmation that it shall notify the customer or subscriber within three days, unless such notice is delayed under the terms of proposed section 2704(c). At this point the provider is also free to notify the subscriber or customer unless prohited under subsection (b) of proposed section 2705

Subsection (a)(3) provides that the provider shall not destroy a back-up copy generated under this section until the latter of the delivery of the information or the resolution of any proceedings related to the access question. If the governmental entity has notified the customer or subscriber and that person has not challenged the requested access then after the passage of fourteen days the provider may make the disclosure. Subsection (a)(5) provides that a governmental entity may only seek to require the creation of a back-up copy under subsection (a)(1) if in its sole discretion there is reason to believe that notification under section 2703 may result in destruction or tampering with the information sought. This determination that notification under section 2703 may result in hampering with or destruction of evidence on similar adverse results by the governmental entity is not subject to challenge by the subscriber or customer or service provider.

Subsection (b)(1) of proposed section 2704 provides that within fourteen days after receipt of notice by the government that a back-up copy has been requested the subscriber or customer may move to quash or vacate. This subsection sets forth the procedural details of such proceedings. The challenger must service the governmental entity and provide written notice to the provider of the challenge. A motion to vacate shall be made in the court which issued the original order. Similarly, a motion to quash shall be made in the appropriate state or federal court. The motion or application under this subsection must establish that the challenger is the relevant customer or subscriber. The challenger must also set forth reasons why the records being sought are not relevant to a legitimate law enforcement inquiry or that some other legal defect exists such as failure by the government to comply with the requirements of this chapter.

Subsection (b)(2) sets forth service of process rules. Service under this section may be made by registered or certified mail to the appropriate governmental entity.

Subsection (b) provides that the government shall be directed to file a sworn response if the challenger has met the requirements of this subsection. The governmental response may be filed *in camera* if appropriate. If the court cannot on the basis of the initial set of papers determine the challenge, then additional proceedings may be conducted. Any additional proceedings and a decision on the challenge shall occur as rapidly as feasible, *i.e.* within 7 calendar days in all but the most unusual circumstances.

Subsection (b)(4) provides that if the court determines that the challenger is not the subscriber or the customer affected does not have legal standing to contest the disclosure then the court shall deny the motion or application. Denial is also directed if the court finds that the information sought is relevant to the legitimate law enforcement inquiry. On the other hand, if the challenger has standing and can show either lack of relevance or non-compliance with the procedural requirements of this section then the court may vacate the order or quash the subpoena.

In the event that there is no indictment then the person whose records are involved may move for the return of the records.

Subsection (b)(5) provides that a court order denying a motion or application under this section shall not be deemed a final order and therefore no interlocutory appeal may be taken from such a denial. Obviously, nothing precludes a customer or subscriber who is later the subject of a criminal proceeding from raising these issues again subject to the sanctions limitation of section 2708.

Proposed section 2705 (a) provides the conditions wherein delay of any required notification may be achieved. Under subsection (a)(1) a governmental entity may request a delay of notification for a period of up to 90 days if the governmental entity convinces the court that there is reason to believe that such notification will produce adverse results as described in subsection (a)(2) of proposed section 2704. Alternatively, where an administrative or grand jury subpoena is obtained, delay may be achieved if a supervisory official files a written certification that such delay is necessary to avoid adverse results. In the second case, the delay in notice can only last initially for a period of up to 90 days.

Subsection (a)(2) sets forth the adverse results which can trigger the delay of notification set out in paragraph (1) of this section. There are five enumerated adverse results: (1) endangering the life or physical safety of an individual; (2) flight from prosecution; (3) destruction of or tampering with evidence; (4) intimidation of potential witnesses (including victims of any crimes); and (5) otherwise seriously jeopardizing an investigation or unduly delaying an ongoing trial.

Subsection (a)(3) requires the government to maintain a true copy of the certification required under paragraph (1)(B) of this section.

Subsection (a)(4) provides that extensions of up to 90 days may be made of the notification so long as the original requirements of this section are met with respect to the extension.

Subsection (a)(5) provides that upon the expiration of any period of delay the governmental entity which has obtained the information shall serve upon the customer or subscriber a copy of the process used to obtain the information. Service under this subsection can be by first class or registered mail. In addition, the government entity must also include a notice that states with reasonable specificity the nature of the law enforcement inquiry. Such notice shall also tell the customer or subscriber when the information was furnished, that the notification was delayed, who authorized the delay and under what provision of law.

Subsection (a)(6) defines, for purposes of this subsection, the term "supervisory official". Such term means the investigative agent or assistant investigative agent in charge or an equivalent official in the investigating agency's headquarters or regional office. The term also means the chief prosecuting attorney or first assistant prosecuting attorney or an equivalent official in a regional or headquarters office.

Subsection (b) of this section provides a procedure for the government to preclude the service provider from notifying the customer or subscriber in a narrow set of circumstances. First, such preclusion may only be obtained in instances where the government is not required to notify, or where the government has obtained the authority to delay notification. Second, a preclusion of notification must be granted by a court of competent jurisdiction. The final requirement is that the court be convinced that there is reason to believe that adverse results set forth in subsection (b) will occur if notification is given.

Sections 2702, 2703 and 2704 affect the contents of communications in storage or where information is being maintained for a subscriber or customer in a remote computing facility. New technologies have created capacities for storage of communications and the single prohibition of interception is not sufficient to cover this record-type aspect of communication. A person who subscribes to an electronic mail service may not realize it, but that service likely maintains a record of all system transactions for a period of time, usually six months under current industry practice. Even if the subscriber reads the message and discards or deletes it, the system maintains it as a backup copy for system maintenance and integrity purposes. These records are retrievable and the Committee intends that subscribers and customers be afforded some protection as to these records. Therefore, a provider of electronic communications to the public such as an electronic mail service may not disclose the contents of stored communications unless one of the statutory exceptions in 2702(b) apply. One of the exceptions, (b)(2), applies where the government has requested access either under section 2703 or 2516.

The Committee has sought to add significant protection to the provision of remote computing services where the contents of communications are electronically transmitted to such service. In most instances, records maintained by third parties have no special privacy or confidentiality protection. The United States Supreme Court has held that an employer's wage records are not subject to the assertion of interest by an employee. *Donaldson v. U.S.*, 400 U.S. 517 (1971). Similarly, in *Miller v. U.S.*, 425 U.S. 435, 1976, the

Court held that an individual has no standing to challenge the disclosure to government of records maintained by banks for their checking account customers. In *Donaldson,* the records sought were the wage records of the employer and were not kept or maintained for the employee. In *Miller,* the bank customer used the bank as an agent to facilitate financial transactions. The records of a checking account were evidence of a public transaction and the disclosure of them to a grand jury did not violate any constitutional rights of bank customers.

These cases were studied extensively by the United States Privacy Protection Study Commission and by the Congress. The Report of the Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977). The Privacy Commission recommended that individuals have enforceable rights to limit the disclosure of records maintained about them for third parties. The Congress acted upon these recommendations in the financial records area by enacting the Right to Financial Privacy Act in 1978. 12 U.S.C. 3400 et seq. That statute in overruling *Miller* requires federal government agencies to use legal process to obtain bank records and allow the bank customer to seek to quash such process.

Last term the Congress extended this type of record privacy protection to records maintained by cable operators. In the Cable Communications Privacy Act of 1984, cable companies in the provision of one-way and two-way services are restricted in the type of information they may disclose about subscribers. Public Law 98-549. Moreover, the legislation, like the Right to Financial Privacy Act, requires the government to obtain records only through a court order or legal process with an opportunity to the subscriber to appear and contest the disclosure of the information.

This Committee is convinced that the subscribers and customers of remote computing services should be afforded a level of confidence that the contents of records maintained on their behalf for the purpose of providing remote computing services will not be disclosed or obtained by the government, unless certain exceptions apply or if the government has used appropriate legal process with the subscribers or customers being given an opportunity to protect their rights.

Proposed section 2706 contains two subsections. Subsection (a) provides that a governmental entity obtaining the contents of communications, records or other transactional information under section 2702, 2703 (with certain exceptions) or 2704 of this title shall pay the person or entity providing such information a fee. The fee under this section shall be reimbursement for such costs as are reasonably necessary and which have been directly incurred in search for, assembly, reproducing or otherwise providing such information. Included in such costs are delivery costs. Also included are any costs due to the necessary disruption of the normal operations of a provider.

Subsection (a) exempts from the reimbursement provisions certain types of records unless the requirement of subsection (c) are met. The type of records involved are telephone toll records and telephone listings. These records are excluded, because for the most part the government has not traditionally paid for such information. Nothing in this exclusion, however, affects the government's

obligation to pay for information through other requests (i.e. requests other than under this chapter). Thus, if a government agent uses a telephone to request information assistance then compensation will be due. Similarly any court appearances in connection with such an information request would be covered elsewhere.

Subsection (b) provides that the amount of the fee provided by subsection (a) of this section shall be either mutually agreed upon or determined by the appropriate court. The subsection specifies which court would be appropriate.

Subsection (c) of proposed section 2703 provides that a court may, upon the request of a person providing information, request an appropriate court to order reimbursement for payment related to expenses incurred in connection with the searching for, reproducing, or transporting books, papers, records, or other information or data required or requested to be produced. *See, e.g.,* 12 U.S.C. 3415. The provider may obtain such reimbursement if the information required is voluminous or otherwise causes an undue burden on the provider. The Committee expects that the Department of Justice will, by regulation (subject to notice and comment), promulgate written criteria to guide the parties and the courts with respect to the meaning of the terms "voluminous" and "undue burden". The Committee hopes that the uniform application of regulations will reduce the need to rely on judicial intervention to resolve reimbursement disputes. The most important factor to examine is the nature of current and past practice in this area. To the extent that the request exceeds the nature and scope of information usually sought without compensation then the reimbursement provisions would come into play.

Proposed Section 2707 contains five subsections. Subsection (a) provides a civil cause of action for any subscriber or customer who has been aggrieved by a knowing or intentional violation of this chapter. Recovery may be had under this section against a person or entity who violated the provisions of this chapter. This includes governmental entities who have violated the provisions of this chapter. Relief as may be appropriate may be awarded under this section but includes preliminary and other equitable relief, declaratory relief, damages and reasonable attorney's fees and other litigation costs reasonably incurred. Subsection (c) provides the measure of damages under this section. Damages include actual damages, any lost profits but in no case less than $1,000.

Subsection (d) sets forth defenses to civil actions. This subsection provides that good faith reliance on a lawful order shall be a complete defense to any civil or criminal action brought under this chapter or any other law. The types of lawful orders are set forth as (1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization, (2) a request of any investigative or law enforcement officer under section 2518(7); or (3) a good faith determination that section 2511(3) of this title permitted the conduct complained of.

Subsection (e) provides the statute of limitations. Under this subsection a civil action may not be commenced later than two years after the date upon which the claimant first discovered or had reasonable opportunity to discover the violation.

Proposed section 2708 provides that the remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter. See discussion of section 101(e) of the bill, *supra.*

Proposed section 2709 contains provisions relating to counterintelligence access to telephone toll and transactional records. Subsection (a) provides that a communications common carrier or an electronic communication service provider shall comply with a request made for telephone subscriber information and toll billing records information or electronic communication transactional records when such a request is made by the Director of the Federal Bureau of Investigation under subsection (b) of this section. Subsection (b) provides that the Director of the FBI (or an individual within the FBI designated for that purpose by the Director) may request any such information and records if there is a certification that the information sought is relevant to an authorized foreign counterintelligence investigation and that there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power (as those terms are defined in the Foreign Intelligence Surveillance Act of 1978).

Subsection (c) provides that a communications common carrier or service provider (including officers, employees and agents) shall not disclose to any person that the FBI has sought or obtained such information or records.

Subsection (d) provides that the FBI may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign counterintelligence collection and foreign counterintelligence investigations conducted by the FBI, with respect to dissemination to an agency of the United States. Any disclosure to a United States agency can only be made if the information is clearly relevant to the authorized responsibilities of such agency.

Subsection (e) provides that the Director of the FBI shall fully inform the House and Senate intelligence committees concerning all requests made under this section.

Proposed section 2910 contains definitions used in this chapter. As a general rule, the terms used in this new chapter have the same definitions as such terms have when used in chapter 119. The term "remote computing service" means "the provision to the public of computer storage or processing services by means of any electronic communication system." Remote computing services is not intended to apply to computer services offered by the various telephone company central offices in connection with the routing of telephone calls (such as speed dialing, call forwarding, and three-way dialing). Computer storage means all types of electronic or magnetic storage, including storage in the memory of a computer.

Section 201(b) contains a clerical amendment to amend the table of chapters to add a new title for chapter 121.

Section 202 of the bill contains the effective date. For this title and the amendments made by this title, the effective date is 90 days after the date of enactment. In the case of conduct pursuant to a court order or extension, it will apply only with respect to court orders or extensions made after this title takes effect.

TITLE III—PEN REGISTERS

This title contains one section and two subsections of the bill. Section 301(a) adds six new sections to title 18 relating to pen registers.

Proposed section 3121 contains three subsections. Subsection (a) contains a general prohibition on pen register use. The subsection provides that no person shall install or use a pen register without first obtaining a court order under section 3123 or under the Foreign Intelligence Surveillance Act.

Subsection (b) contains exceptions to the general list of prohibitions. The subsection provides that the prohibitions do not apply with respect to the use of a pen register by a provider of electronic or wire communication service if either of two conditions are met. The first condition is that such use relates to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of the service or unlawful use of service.

The second permissible condition for the use of a pen register is to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or user of that service, from fraudulent, unlawful or abusive use of service, or with the consent of the user of that service.

Subsection (c) provides that penalty for knowingly violating subsection (a). The penalty is a fine under this title or imprisonment of up to one year, or both.

The absence of any specific civil cause of action for violations of proposed chapter 206 was purposeful; therefore, no private cause of action should be implied under this chapter.

Proposed section 3122 provides the procedures for making an application for a pen register order. Under subsection (a) an attorney for the government may make an application for an order or an extension of an order authorizing or approving the installation and use of pen registers. The application shall be in writing under oath or equivalent affirmation to a court of competent jurisdiction. Subsection (a)(2) contains parallel provisions with respect to state applications. The phrase ". . . unless otherwise prohibited by State law" in this subsection makes clear that this law does not preempt any existing state laws with respect to installation and use of pen registers by state officials. To the extent that state law currently provides that a pen register may only be installed or used by a state official based on some other, higher standard of proof, that law will continue in effect with respect to such officials. *See People* v. *Sporleder,* 666 P. 2d 135 (Colo. Sup. Ct. 1983); Note, On Privacy, Pen Registers, and State Constitutions: The Colorado Supreme Court Rejects *Smith* v. *Maryland,* 15 Tol L. Rev. 1466 (1984); *People* v. *McCunes,* 51 Cal. App. 3d 487 (1975). Subsection (b) provides what factual details need to be provided in the application. The application shall include the identity of the attorney for the federal or state government and the identity of the applicant making the application, and a certification by the applicant that the information

likely to be obtained is relevant to an ongoing criminal investigation being conducted by the agency.

Proposed section 3123 contains four subsections. Subsection (a) provides that upon an application the court shall issue an *ex parte* order authorizing the installation and use of a pen register within the jurisdiction of the court if the court finds that the government attorney has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. This provision does not envision an independent judicial review of whether the application meets the relevance standard rather the court needs only to review the completeness of the submitted certification.

Subsection (b) sets forth the contents of the order for a pen register, authorization or installation. The order is required to specify (1) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register is attached; (2) the identity, if known, of the person who is the subject of the criminal investigation; (3) the number and, if known, physical location of the telephone line to which the pen register is attached; and (4) a statement of the offense to which the information likely to be obtained by the pen register relates. In addition, the order shall direct, upon request, the furnishing of information facilities and technical assistance necessary to accomplish the installation of the pen register. The content of the order relating to cooperation is intended to codify the existing informal practice of cooperation between the telephone companies and the Department of Justice.

Subsection (c) provides that the time period of authorization of an installation and use of a pen register is 60 days, with possible extensions of 60 days.

Subsection (d) provides that an order authorizing or approving the installation and use of a pen register shall direct that the order be sealed, until otherwise ordered by the court. In addition, the order shall bar the disclosure of the existence of a pen register or an investigation to the listed subscriber, or to any other unauthorized person, unless or until otherwise directed by the court. Intentional violations of the non-disclosure provisions may be, in appropriate circumstances, punishable as contempt.

Proposed section 3124 contains two subsections. Subsection (a) provides that upon the request of an authorized person a provider of a wire communication service, landlord, custodian, or other person shall furnish such person with all information, facilities, and technical assistance necessary to effectuate the order unobtrusively and with a minimum of interference. The Committee assumes that the current practice of law enforcement officials installing and maintaining the pen register will continue. Subsection (b) provides that the persons giving assistance under this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance. This compensation provision is modeled after that which applies under chapter 119 of title 18 and is intended to be interpreted and implemented in a similar fashion.

Proposed section 3125 provides that the Attorney General shall annually report to the Congress on the number of pen register

orders applied for by law enforcement agencies of the Department of Justice. Under a current order of the Attorney General statistics concerning pen registers are compiled. Memorandum from Assistant Attorney General, Criminal Division, Department of Justice, Phillip B. Heyman to all Investigative Agencies, dated Sept. 24, 1979 (Recording the number of investigations, number of persons affected and nature of the offenses). This section merely requires that this information be reformulated and submitted to the appropriate committees of the Congress. Obviously the greater the detail contained in these reports the less need there will be for supplemental activities. Therefore, it would be helpful to the Committee if these reports could indicate for which offenses pen registers are being used.

Proposed section 3126 contains definitions for this chapter. Subsection (a) contains the definitions. The term "communications common carrier" has the same meaning as is found in section 3(h) of the Communications Act of 1934. The term "wire communication" has the meaning set forth in section 2510 of this title. The term "court of competent jurisdiction" means a district court of the United States (including a magistrate of such court) or a United States Court of Appeals or a court of general jurisdiction of a State authorized to enter orders authorizing the use and installation of pen registers. The term "pen register" means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted for purposes of routing telephone calls, with respect to wire communications, on the telephone line to which such device is attached. The term does not include the contents of a communication, rather it records the numbers dialed. Such term does not include any device used by a provider of wire communication service for billing, or recording as incident to billing, for communications services provided by such provider. The term "attorney for the government" has the meaning given to that term by the Federal Rules of Criminal Procedure. The term "state" means a State, the District of Columbia, Puerto Rico, and other possession or territory of the United States.

Subsection (b) of this section contains a clerical amendment amending the table of chapters.

Section 302 contains the effective date. Subsection (a) provides that as a general rule the amendments made by this title shall take effect 90 days after enactment. In addition, in the case of conduct pursuant to a court order or extension, these amendments apply only with respect to court orders or extensions made after the title takes effect.

Subsection (b) contains special rules or exceptions. This subsection, in essence, gives states two years to bring their laws into conformity with these amendments to federal law.

New Budget Authority

In regard to clause (l)(3)(B) of rule XI of the Rules of the House of Representatives, the bill creates no new budget authority or increased tax expenditures for the Federal judiciary.

INFLATIONARY IMPACT STATEMENT

In regard to clause 2(l)(4) of rule XI of the Rules of the House of Representatives, the commitee feels that the bill will have no foreseeable inflationary impact on prices or costs in the operation of the national economy.

FEDERAL ADVISORY COMMITTEE ACT OF 1972

The Committee finds that this legislation does not create any new advisory committees within the meaning of the Federal Advisory Committee Act of 1972.

COST ESTIMATE

In compliance with clause 7 of rule XIII of the Rules of the House of Representatives, the committee estimates that the costs which will be incurred in carrying out the provisions of the reported bill are accurately reflected in the Congressional Budget Office estimate.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, June 18, 1986.

Hon. PETER W. RODINO, Jr.,
Chairman, Committee on the Judiciary, House of Representatives, Rayburn Office Building, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has reviewed H.R. 4952, the Electric Communications Privacy Act of 1986, as ordered reported by the House Committee on the Judiciary, June 10, 1986. CBO estimates that enactment of this legislation will result in no significant cost to the federal government and no cost to state or local governments.

H.R. 4952 makes a number of amendments to Title 18 of the United States Code concerning access to electronic communications. Title I of the bill establishes penalties for the unlawful interception or disclosure of electronic communications, provides for the recovery of civil damages for persons whose communications are intercepted, disclosed or used in violation of this provision, and modifies procedures for government interception of communications. Title II creates specific penalties for unlawful access to stored wire and electronic communications, while Title III establishes a general prohibition on the use of pen registers. These titles include specific procedures for access to stored communications and use of pen registers by government entities, and Title II includes a provision for civil actions.

H.R. 4952 requires government entities to compensate private parties assembling or providing information concerning stored electronic communications, or assisting in the installation and use of a pen register. Because such compensation is currently provided in Department of Justice investigations, CBO does not expect these provisions to involve any significant additional cost for the federal government.

Based on information from the Department of Justice, we do not expect enactment of this bill to result in a significant change in the government's law enforcement practices or expenditures. H.R. 4952 would provide a specific foundation in the code for current law enforcement efforts the Department is undertaking under other authority.

If you wish further details on this estimate, we will be pleased to provide them.

With best wishes,
Sincerely,

RUDOLPH G. PENNER, *Director.*

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3 of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

TITLE 18, UNITED STATES CODE

PART I—CRIMES

CHAPTER 109—SEARCHES AND SEIZURES

• • • • • • •

§ 2232. Destruction or removal of property to prevent seizure

(a) PHYSICAL INTERFERENCE WITH SEARCH.—Whoever, before, during, or after seizure of any property by any person authorized to make searches and seizures, in order to prevent the seizure or securing of any goods, wares, or merchandise by such person, staves, breaks, throws overboard, destroys, or removes the same, shall be fined not more than $10,000 or imprisoned more than five years, or both.

(b) NOTICE OF SEARCH.—Whoever, having knowledge that any person authorized to make searches and seizures has been authorized or is otherwise likely to make a search or seizure, in order to prevent the authorized seizing or securing of any person, goods, wares, merchandise or other property, gives notice or attempts to give notice of the possible search or seizure to any person shall be fined not more than $10,000 or imprisoned not more than five years, or both.

(c) NOTICE OF CERTAIN ELECTRONIC SURVEILLANCE.—Whoever, having knowledge that a Federal investigative or law enforcement

officer has been authorized or has applied for authorization under chapter 119 to intercept a wire, oral, or electronic communication, in order to obstruct, impede, or prevent such interception, gives notice or attempts to give notice of the possible interception to any person shall be fined under this title or imprisoned not more than five years, or both.

Whoever, having knowledge that a Federal officer has been authorized or has applied for authorization to conduct electronic surveillance under the Foreign Intelligence Surveillance Act (50 U.S.C. 1801, et seq.), in order to obstruct, impede, or prevent such activity, gives notice or attempts to give notice of the possible activity to any person shall be fined under this title or imprisoned not more than five years, or both.

* * * * * * *

CHAPTER 119—WIRE *AND ELECTRONIC COMMUNICATIONS* INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS

Sec.
2510. Definitions.

* * * * * * *

2521. Injunction against illegal interception.

§ 2510. Definitions

As used in this chapter—

(1) "wire communication" means any [communication] *aural transfer* made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception *(including the use of such connection in a switching station)* furnished or operated by any person engaged [as a common carrier] in providing or operating such facilities for the transmission of interstate or foreign communications *or communications affecting interstate or foreign commerce, but such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;*

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, *but such term does not include any electronic communication;*

* * * * * * *

(4) "intercept" means the aural *or other* acquisition of the contents of any wire, *electronic,* or oral communication through the use of any electronic, mechanical, or other device.

(5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire [or oral], *oral, or electronic* communication other than—

(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a [communications common carrier]

provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business; or (ii) being used by a communications common carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

* * * * * * *

(8) "contents", when used with respect to any wire [or oral], *oral, or electronic* communication, includes any information concerning the [identity of the parties to such communication or the existence,] substance, purport, or meaning of that communication;

(9) "Judge of competent jursidiction" means—

(a) a judge of a United States district court or a United States court of appeals; and

(b) a judge of any court of general criminal jurisdiction of a State who is authorized by a statute of that State to enter orders authorizing interceptions of wire [or oral], *oral, or electronic* communications;

(10) "communication common carrier" shall have the same meaning which is given the term "common carrier" by section 153(h) of title 47 of the United States Code; [and]

(11) "aggrieved person" means a person who was a party to any intercepted wire [or oral], *oral, or electronic* communication or a person against whom the interception was directed[.];

(12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

(A) the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit;

(B) any wire or oral communication;

(C) any communication made through a tone-only paging device; or

(D) any communication from a tracking device (as defined in section 3117 of this title);

(13) "user" means any person or entity who—

(A) uses an electronic communication service; and

(B) is duly authorized by the provider or such service to engage in such use;

(14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;

(16) "readily accessible to the general public" means, with respect to a radio communication, that such communication is not—

(A) scrambled or encrypted;

(B) transmitted using modulation techniques whose essential parameters have been withheld from the public with the intention of preserving the privacy of such communication;

(C) carried on a subcarrier or other signal subsidiary to a radio transmission;

(D) transmitted over a communication system provided by a common carrier, unless the communication is a tone only paging system communication; or

(E) transmitted on frequencies allocated under part 25, subpart D, E, or F of part 74, or part 94 of the Rules of the Federal Communications Commission, unless, in the case of a communication transmitted on a frequency allocated under part 74 that is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio;

(17) "electronic storage" means—

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication; and

(18) "aural transfer" means a transfer containing the human voice at any point between and including the point of origin and the point of reception.

§ 2511. Interception and disclosure of wire or oral communications prohibited

(1) Except as otherwise specifically provided in this chapter any person who—

(a) willfully intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire [or oral] *oral, or electronic* communication;

(b) willfully uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—

(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or

(ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

(iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or

(iv) such use or endeavor to use (A) takes place on the permises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or

(v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

(c) willfully discloses, or endeavors to disclose, to any other person the contents of any wire [or oral] *oral, or electronic* communication, knowing or having reason to know that the information was obtained through the interception of a wire [or oral] *oral, or electronic* communication in violation of this subsection; or

(d) willfully uses, or endeavors to use, the contents of any wire [or oral] *oral, or electronic* communication, knowing or having reason to know that the information was obtained through the interception of a wire [or oral] *oral, or electronic* communication in violation of this subsection; [shall be fined not more than $10,000 or imprisoned not more than five years, or both.] *shall be punished as provided in subsection (4).*

(2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of [any communication common carrier,] *a provider of wire or electronic communication service,* whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property [of the carrier of such communication: *Provided,* That said communication common carriers] *of the provider of that service, except that a provider of wire communication service to the public* shall not utilize service observing or random monitoring except for mechanical or service qualtiy control checks.

(ii) Notwithstanding any other law, *providers of wire or electronic communication service,* [communication common carriers,]their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information facilities, or technical assistance to persons authorized by law to intercept wire [or oral] , *oral, or electronic* communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if [the common carrier,] *such provider* its officers, employees, or agents, landlord, custodian, or other specified person has been provided with—

(A) a court order directing such assistance signed by the authorizing judge, or

(B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required.

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No [communication common carrier] *provider of wire or*

electronic communication service officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished an order or certification under this subparagraph, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any violation of this subparagraph by a [communication common carrier] *provider of wire or electronic communication service* or an officer, employee, or agent thereof, shall render the carrier liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any [communication common carrier] *provider of wire or electronic communication service* its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of an order or certification under this subparagraph.

(b) It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire *or electronic* communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire [or oral], *oral, or electronic* communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire [or oral], *oral, or electronic* communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the pupose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State [or for the purpose of committing any other injurious act].

(e) Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an office, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f) Nothing contained in this chapter *or chapter 121,* or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communication [by], *or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing* a means other than electronic

surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire and oral communications may be conducted.

(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—

(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted—

(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;

(II) by any governmental, law enforcement, civil defense, or public safety communications system, including police and fire, readily accessible to the general public;

(III) by a station operating on a frequency assigned to the amateur, citizens band, or general mobile radio services; or

(IV) by any marine or aeronautical communications system;

(iii) to engage in any conduct which—

(I) is prohibited by section 633 of the Communications Act of 1934; or

(II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station, to the extent necessary to identify the source of such interference; or

(v) for other users of the same frequency to intercept any radio communication made through a common carrier system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled encrypted.

(h) It shall not be unlawful under this chapter—

(i) to use a pen register (as that term is defined for the purpose of chapter 206 (relating to pen registers) of this title);

(ii) for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service; or

(iii) to use a device that captures the incoming electronic or other impulses which identify the numbers of an instrument from which a wire communication was transmitted.

(3)(A) Except as provided in subparagraph (B) of this paragraph, a person or entity providing an electronic communication service to the public shall not willfully divulge the contents of any communication (other than one to such person or entity, or an agent thereof)

while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(B) A person or entity providing electronic communication service to the public may divulge the contents of any such communication—

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)(a) Except as provided in paragraph (b) of this subsection, whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

(b) If the offense is a first offense under paragraph (a) of this subsection and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication, then—

(i) if the communication is not the radio portion of a cellular telephone communication, the offender shall be fined under this title or imprisoned not more than one year, or both; and

(ii) if the communication is the radio portion of a cellular telephone communication, the offender shall be fined not more than $500 or imprisoned not more than six months, or both.

(c) Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted to a broadcasting station for purposes of retransmission to the general public is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

§ 2512. Manufacture, distribution, possession, and advertising of wire or oral communication intercepting devices prohibited

(1) Except as otherwise specifically provided in this chapter, any person who willfully—

(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire [or oral], *oral, or electronic* communications;

(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire [or oral], *oral, or electronic* communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c) places in any newspaper, magazine, handbill, or other publication any advertisement of—

(i) any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire [or oral], *oral, or electronic* communications; or

(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire [or oral], *oral, or electronic* communications,

knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce,

shall be fined not more than $10,000 or imprisoned not more than five years, or both.

(2) It shall not be unlawful under this section for—

(a) [a communications common carrier] *a provider of wire or electronic communication service* or an officer, agent, or employee of, or a person under contract with, [a communications common carrier] *such a provider,* in the normal course of the [communications common carrier's business] *business of providing that wire or electronic communication service,* or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire [or oral], *oral, or electronic* communications.

§ 2513. Confiscation of wire [or oral], *oral, or electronic* communication intercepting devices

Any electronic, mechanical, or other device used, sent, carried, manufactured, assembled, possessed, sold, or advertised in violation of section 2511 or section 2512 of this chapter may be seized and forfeited to the United States. All provisions of law relating to (1) the seizure, summary and judicial forfeiture, and condemnation of vessels, vehicles, merchandise, and baggage for violations of the customs laws contained in title 19 of the United States Code, (2) the disposition of such vessels, vehicles, merchandise, and baggage or the proceeds from the sale thereof, (3) the remission or mitigation of such forfeiture, (4) the compromise of claims, and (5) the award of compensation to informers in respect of such forfeitures, shall apply to seizures and forfeitures incurred, or alleged to have been incurred, under the provisions of this section, insofar as applicable and not inconsistent with the provisions of this section; except that such duties as are imposed upon the collector of customs or any other person with respect to the seizure and forfeiture of vessels, vehicles, merchandise, and baggage under the provisions of the customs laws contained in title 19 of the United States Code shall be

performed with respect to seizure and forfeiture of electronic, mechanical, or other intercepting devices under this section by such officers, agents, or other persons as may be authorized or designated for that purpose by the Attorney General.

§ 2515. Prohibition of use as evidence of intercepted wire [or oral], *oral, or electronic* communications

Whenever any wire [or oral], *oral, or electronic* communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

§ 2516. Authorization for interception of wire [or oral], *oral, or electronic* communications

(1) The Attorney General, Deputy Attorney General, Associate Attorney General, [or] any Assistant Attorney General, *any acting Assistant Attorney General, or any Deputy Assistant Attorney General in the Criminal Division* specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of—

(a) any offense punishable by death or by imprisonment for more than one year under sections 2274 through 2277 of title 42 of the United States Code (relating to the enforcement of the Atomic Energy Act of 1954), or under the following chapters of this title: chapter 37 (relating to espionage), chapter 105 (relating to sabotage), chapter 115 (relating to treason), or chapter 102 (relating to riots);

(b) a violation of section 186 or section 501(c) of title 29, United States Code (dealing with restrictions on payments and loans to labor organizations), or any offense which involves murder, kidnapping, robbery, or extortion, and which is punishable under this title;

(c) any offense which is punishable under the following sections of this title: section 201 (bribery of public officials and witnesses), section 224 (bribery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1084 (transmission of wagering information), *section 751 (relating to escape)*, sections 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1751 (Presidential and Presidential staff assassination, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises),

section 1952A (relating to use of interstate commerce facilities in the commission of murder for hire), section 1952B (relating to violent crimes in aid of racketeering activity), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), section 1343 (fraud by wire, radio, or television), section 2252 or 2253 (sexual exploitation of children), sections 2251 and 2252 (sexual exploitation of children), sections [2314] *2312, 2313, 2314*, and 2315 (interstate transportation of stolen property), *the second section 2320 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3) (relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities)*, section 1963 (violations with respect to racketeer influenced and corrupt organizations), *section 115 (relating to threatening or retaliating against a Federal official), the section in chapter 65 relating to destruction of an energy facility, and section 1341 (relating to mail fraud)*, or section 351 (violations with respect to congressional, Cabinet, or Supreme Court assassination, kidnapping, and assault);

(d) any offense involving counterfeiting punishable under section 471, 472, or 473 of this title;

(e) any offense involving fraud connected with a case under title 11 or the manufacture, importation, receiving, concealment, buying, selling, or otherwise dealing in narcotic drugs, marihuana, or other dangerous drugs, punishable under any law of the United States;

(f) any offense including extortionate credit transactions under sections 892, 893, or 894 of this title;

(g) a violation of section 5322 of title 31, United States Code (dealing with the reporting of currency transactions); [or]

(h) any felony violation of sections 2511 and 2512 (relating to interception and disclosure of certain communications and to certain devices) of this title;

(i) the location of any fugitive from justice from an offense described in this section; or

[(h)] *(j)* any conspiracy to commit any of the foregoing offenses.

(2) The principal prosecuting attorney of any State, or the principal prosecuting attorney of any political subdivision thereof, if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction for an order authorizing or approving the interception of wire [or oral], *oral, or electronic* communications, may apply to such judge for, and such judge may grant in conformity with section 2518 of this chapter and with the applicable State statute an order authorizing, or approving the interception of wire [or oral], *oral, or electronic* communications by investigative or law enforcement officers having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of the commission of the offense of murder, kidnapping, gambling, robbery, bribery, extortion, or deal-

ing in narcotic drugs, marihuana or other dangerous drugs, or other crime dangerous to life, limb, or property, and punishable by imprisonment for more than one year, designated in any applicable State statute authorizing such interception, or any conspiracy to commit any of the foregoing offenses.

(3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony.

§ 2517. Authorization for disclosure and use of intercepted wire [or oral], *oral, or electronic* communications

(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire [or oral], *oral, or electronic* communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire [or oral], *oral, or electronic* communication or evidence derived therefrom any use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter, any information concerning a wire [or oral], *oral, or electronic* communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

(4) No otherwise privileged wire [or oral], *oral, or electronic* communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

(5) When an investigative or law enforcement officer, while engaged in intercepting wire or oral communications in the manner authorized herein, intercepts wire [or oral], *oral, or electronic* communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable.

§ 2518. Procedure for interception of wire [or oral], *oral, or electronic* communications

(1) Each application for an order authorizing or approving the interception of a wire [or oral], *oral, or electronic* communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information:

(a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application;

(b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) *except as provided in subsection (11),* a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted;

(c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatially terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter;

(e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire [or oral], *oral, or electronic* communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and

(f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application.

(3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving inteception of wire [or oral], *oral, or electronic* communications within the territorial jurisdiction of the court in which the judge is sitting *(and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction) after within the territorial jurisdiction of the*

court in which the judge is sitting, if the judge determines on the basis of the facts submitted by the applicant that—

(a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter.

(b) there is probable cause for brief that particular communications concerning that offense will be obtained through such interception;

(c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;

(d) *except as provided in subsection (11),* there is probable cause for belief that the facilities from which, or the place where, the wire [or oral], *oral, or electronic* communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

(4) Each order authorizing or approving the interception of any wire [or oral], *oral, or electronic* communication under this chapter shall specify—

(a) the identity of the person, if known, whose communications are to be intercepted;

(b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted;

(c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates;

(d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and

(e) the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

An order authorizing the interception of a wire [or oral], *oral, or electronic* communication under this chapter shall, upon request of the applicant, direct that a [communication common carrier,] *provider of electronic communication service,* landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such carrier, landlord, custodian, or person is according the person whose communications are to be intercepted. Any communication common carrier, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant [at the prevailing rates.] *for reasonable expenses incurred in providing such facilities or assistance.*

(5) No order entered under this section may authorize or approve the interception of any wire [or oral], *oral, or electronic* communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. *Such thirty-day period begins on the earlier of the day on which the*

investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise, subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. *In the event the intercepted communications is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception.*

(6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.

(7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that—

(a) an emergency situation exists that involves—

(i) immediate danger of death or serious physical injury to any person.

(ii) conspiratorial activities threatening the national security interest, or

(iii) conspiratorial activities characteristic of organized crime,

that requires a wire [or oral], *oral, or electronic* communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and

(b) there are grounds upon which an order could be entered under this chapter to authorize such interception,

may intercept such wire [or oral], *oral, or electronic* communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception

is terminated without an order having been issued, the contents of any wire [or oral], *oral, or electronic* communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application.

(8)(a) The contents of any wire [or oral], *oral, or electronic* communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire [or oral], *oral, or electronic* communication under this subsection shall be done in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under this directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years. Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire [or oral], *oral, or electronic* communication or evidence derived therefrom under subsection (3) of section 2517.

(b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.

(c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge.

(d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518(7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of—

(1) the fact of the entry of the order or the application;

(2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and

(3) the fact that during the period wire [or oral], *oral, or electronic* communications were or were not intercepted.

The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed.

(9) The contents of any wire [or oral], *oral, or electronic* communication intercepted pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information.

(10)(a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that—

(i) the communication was unlawfully intercepted;

(ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or

(iii) the interception was not made in conformity with the order of authorization or approval.

Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice.

(b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted.

(c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications.

(11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if—

(i) in the case of an application with respect to the interception of an oral communication—

(I) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General,

the Deputy Attorney General, the Associate Attorney General an Assistant Attorney General, or an acting Assistant Attorney General;

(II) the application contains a full and complete statement as to why such specification is not practical and identifies the person committing the offense and whose communications are to be intercepted; and

(III) the judge finds that such specification is not practical; and

(ii) in the case of an application with respect to a wire or electronic communication—

(I) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General;

(II) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing of a purpose, on the part of that person, to thwart interception by changing facilities; and

(III) the judge finds that such purpose has been adequately shown.

(12) An interception of a communication under an order with respect to which the requirements of subsections (1)(b)(ii) and (3)(d) of this section do not apply by reason of subsection (11) shall not begin until the facilities from which, or the place where, the communication is to be intercepted is ascertained by the person implementing the interception order.

§ 2519. Reports concerning intercepted wire [or oral], *oral, or electronic* communications

(1) Within thirty days after the expiration of an order (or each extension thereof) entered under section 2518, or the denial of an order approving an interception, the issuing or denying judge shall report to the Administrative Office of the United States Courts—

(a) the fact that an order or extension was applied for;

(b) the kind of order or extension applied for *(including whether or not the order was an order with respect to which the requirements of sections 2518(1)(b)(ii) and 2518(3)(d) of this title did not apply by reason of section 2518(11) of this title)*;

(c) the fact that the order or extension was granted as applied for, was modified, or was denied;

(d) the period of interceptions authorized by the order, and the number and duration of any extensions of the order;

(e) the offense specified in the order or application, or extension or an order;

(f) the identity of the applying investigative or law enforcement officer and agency making the application and the person authorizing the application; and

(g) the nature of the facilities from which or the place where communications were to be intercepted.

(2) In January of each year the Attorney General, an Assistant Attorney General specially designated by the Attorney General, or the principal prosecuting attorney of a State, or the principal prosecuting attorney for any political subdivision of a State, shall report to the Administrative Office of the United States Courts—

(a) the information required by paragraphs (a) through (g) of subsection (1) of this section with respect to each application for an order or extension made during the preceding calendar year;

(b) a general description of the interceptions made under such order or extension, including (i) the approximate nature and frequency of incriminating communications intercepted, (ii) the approximate nature and frequency of other communications intercepted, (iii) the approximate number of persons whose communications were intercepted, and (iv) the approximate nature, amount, and cost of the manpower and other resources used in the interceptions;

(c) the number of arrests resulting from interceptions made under such order or extension, and the offenses for which arrests were made;

(d) the number of trials resulting from such interceptions;

(e) the number of motions to suppress made with respect to such interceptions, and the number granted or denied;

(f) the number of convictions resulting from such interceptions and the offenses for which the convictions were obtained and a general assessment of the importance of the interceptions; and

(g) the information required by paragraphs (b) through (f) of this subsection with respect to orders or extensions obtained in a preceding calendar year.

(3) In April of each year the Director of the Administrative Office of the United States Courts shall transmit to the Congress a full and complete report concerning the number of applications for orders authorizing or approving the interception of wire [or oral], *oral, or electronic* communications pursuant to this chapter and the number of orders and extensions granted or denied pursuant to this chapter during the preceding calendar year. Such report shall include a summary and analysis of the data required to be filed with the Administrative Office by subsections (1) and (2) of this section. The Director of the Administrative Office of the United States Courts is authorized to issue binding regulations dealing with the content and form of the reports required to be filed by subsections (1) and (2) of this section.

§ 2520. Recovery of civil damages authorized

[Any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter shall (1) have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications, and (2) be entitled to recover from any such person—

[(a) actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher;

[(b) punitive damages; and

[(c) a reasonable attorney's fee and other litigation costs reasonably incurred.

A good faith reliance on a court order or legislative authorization shall constitute a complete defense to any civil or criminal action brought under this chapter or under any other law.]

§ 2520. Recovery of civil damages authorized

(a) IN GENERAL.—Any person whose wire, oral, or electronic communication is intercepted, disclosed, or willfully used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

(b) RELIEF.—In an action under this section appropriate relief includes—

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (c) and punitive damages in appropriate cases; and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) COMPUTATION OF DAMAGES.—The court may assess as damages in an action under this section whichever is the greater of—

(1) the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation; or

(2) statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000.

(d) DEFENSE.—A good faith reliance on—

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense against any civil or criminal action brought under this chapter or any other provision of law.

(e) LIMITATION.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first has a reasonable opportunity to discover the violation.

§ 2521. Injunction against illegal interception

Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this chapter, the Attorney General may initiate a civil action in a district court of the United States to enjoin such violation. The court shall proceed as soon as practicable to the hearing and determination of such an action, and may, at any time before final determination, enter such a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the United States or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Federal Rules of Civil Procedure, except that, if an indictment has been returned against the respondent, discovery is governed by the Federal Rules of Criminal Procedure.

CHAPTER 121—STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

§ 2701. Unlawful access to stored communications

(a) OFFENSE.—Except as provided in subsection (c) of this section whoever—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communications while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) PUNISHMENT.—The punishment for an offense under subsection (a) of this section is—

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain—

(A) a fine of not more than $250,000 or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than two years, or both, for any subsequent offense under this subparagraph; and

(2) a fine of not more than $5,000 or imprisonment for not more than six months, or both, in any other case.

(c) EXCEPTIONS.—Subsection (a) of this section does not apply with respect to conduct authorized—

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703 or 2704 of this title.

§ 2702. Disclosure of contents

(a) PROHIBITIONS.—Except as provided in subsection (b)—

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity

the contents of any communication which is carried or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(b) EXCEPTIONS.—A person or entity may divulge the contents of a communication—

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2516, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or

(6) to a law enforcement agency, if such contents—

(A) were inadvertently obtained by the service provider; and

(B) appear to pertain to the commission of a crime.

§ 2703. Requirements for governmental access

(a) CONTENTS OF ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a non-voice wire communication or an electronic communication, that is in electronic storage in an electronic communications system for 180 days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than 180 days by the means available under subsection (b) of this section.

(b) CONTENTS OF ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) Without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscribe or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) RECORDS CONCERNING ELECTRONIC COMMUNICATIONS SERVICE OR REMOTE COMPUTING SERVICE.—A governmental entity may require a provider of electronic communications service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) without required notice to the subscriber or customer if the governmental entity—

(1) uses an administrative subpoena authorized by a Federal or State statute, or a Federal or State grand jury subpoena;

(2) obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant; or

(3) obtains a court order for such disclosure under subsection (d) of this section.

(d) REQUIREMENTS FOR COURT ORDER.—A court order for disclosure under subsection (b) or (c) of this section shall issue only if the governmental entity shows that there is reason to believe the contents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State.

§ 2704. Backup preservation

(a) BACKUP PRESERVATION.—(1) A governmental entity acting uinder section 2703(b)(2) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subcriber or customer of such subpoena or court order, such service provider shall create such backup copy as soon as practicalbe consistent with its regular business practices and shall confirm to the governmental entrity that such backup copy has been

made. Such backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

(2) Notice to the subscriber or customer shall be made by the governmental entity within three days after receipt of such confirmation, unless such notice is delayed pursuant to section 2705(a).

(3) The service provider shall not destroy such backup copy until the later of—

(A) the delivery of the information; or

(B) the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order.

(4) The service provider shall release such backup copy to the requesting governmental entity no sooner than 14 days after the governmental entity's notice to the subscriber or customer if such service provider—

(A) has not received notice from the subscriber or customer that the subscriber or customer has challenged the governmental entity's request; and

(B) has not initiated proceedings to challenge the request of the government entity.

(5) A governmental entity may seek to require the creation of a backup copy under subsection (a)(1) of this section if in its sole discretion such entity determines that there is reason to believe that notification under section 2703 of this title of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determiantion is not subject to challenge by the subscriber or customer or service provider.

(b) CUSTOMER CHALLENGES.—(1) Within 14 days after notice by the governmental entity to the subscriber or customer under subsection (a)(2) of this section, such subscriber or customer may file a motion to quash such subpoena or vacate such court order, with copies served upon the governmental entity and with written notice of such challenge to the service provider. A motion to vacate a court order shall be filed in the court which issued such order. A motion to quash a subpoena shall be filed in the appropriate United States district or State court. Such motion or application shall contain an affidavit or sworn statement—

(A) stating that the applicant is a customer or subscriber to the service from which the contents of electronic communications maintained for him have been sought; and

(B) stating the applicant's reasons for believing that the records sought are not relevant to a legitimate law enforcement inquiry or that there has not been substantial compliance with the provisions of this chapter in some other respect.

(2) Service shall be made under this section upon a governmental entity by delivering or mailing by registered or certified mail a copy of the papers to the person, office, or department specified in the notice which the customer has received pursuant to this chapter. For the purposes of this section, the term "delivery" has the meaning given that term in the Federal Rules of Civil Procedure.

(3) If the court finds that the customer had complied with paragraphs (1) and (2) of this subsection, the court shall order the governmental entity to file a sworn response, which may be filed in camera if the governmental entity includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and response, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or applications decided as soon as practicable after the filing of the governmental entity's response.

(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the governmental entity are maintained, or that there is a reason to believe that the law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order such process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not a reason to believe that the communications sought are relevant to a legitimate law enforcement inquiry, or that there has not been substantial compliance with the provisions of this chapter, it shall order the process quashed.

(5) A court order denying a motion or application under this section shall not be deemed a final order and no interlocutory appeal may be taken therefrom by the customer.

§ 2705. Delayed notice

(a) DELAY OF NOTIFICATION.—(1) A governmental entity acting under section 2703(b) of this title may—

(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed 90 days; if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed 90 days upon the execution a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

(2) An adverse resut for the purposes of paragraph (1) of this subsection is—

(A) endangering the life or physical safety of an individual;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

(4) Extensions of the delay of notification provided in section 2703 of up to 90 days each may be granted by the court upon application,

or by certification by a governmental entity, but only in accordance with subsection (b) or (c) of this section.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first class mail to, the customer or subscriber a copy of the process or request together with notice that—

(A) states with reasonable specificity the nature of the law enforcement inquiry; and

(B) informs such customers or subscriber—

(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

(ii) that notification of such customer or subscriber was delayed;

(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

(iv) which provision of this chapter allowed such delay.

(6) As used in this subsection, the term "supervisory official" mans the investigtive agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

(b) PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENTAL ACCESS.—A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in—

(1) endangering the life or physical safety of an individual;

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

§ 2706. Cost reimbursement

(a) PAYMENT.—Except as otherwise provided in subsection (c), a governmental entity obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704 of this title shall pay to the person or entity assembling or providing such information a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information. Such reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which such information may be stored.

(b) AMOUNT.—The amount of the fee provided by subsection (a) shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court which issued the order for production of such information (or the court before which a criminal prosecution relating to such information would be brought, if no court order was issued for production of the information).

(c) The requirement of subsection (a) of this section does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703 of this title. The court may, however, order a payment as described in subsection (a) if the court determines the information required is unusually voluminous in nature or otherwise caused an undue burden on the provider.

§ 2707. Civil Action

(a) CAUSE OF ACTION.—Any provider of electronic communication service, subscriber, or customer aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action recover from the person or entity which engaged in that violation such relief as may be appropriate.

(b) RELIEF.—In a civil action under this section, appropriate relief includes—

(1) such preliminary and other equitable or declaratory relief as may be appropriate;

(2) damages under subsection (3); and

(3) a reasonable attorney's fee and other litigation costs reasonably incurred.

(c) DAMAGES.—The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000.

(d) DEFENSE.—A good faith reliance on—

(1) a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 2518(7) of this title; or

(3) a good faith determination that section 2511(3) of this title permitted the conduct complained of;

is a complete defense to any civil or criminal action brought under this chapter or any other law.

(e) LIMITATION.—A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

§ 2708. Exclusivity of remedies

The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.

§ 2709. Counterintelligence access to telephone toll and transactional records

(a) DUTY TO PROVIDE.—A Communications common carrier or an electronic communication service provider shall comply with a request made for telephone subscriber information and toll billing information, or electronic communication transactional records made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) REQUIRED CERTIFICATION.—The Director of the Federal Bureau of Investigation (or an individual within the Federal Bureau of Investigation designated for this purpose by the Director) may request any such information and records if the Director (or the Director's designee) certifies in writing to the carrier or provider to which the request is made that—

(1) the information sought is relevant to an authorized foreign counterintelligence investigation; and

(2) there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801).

(c) PROHIBITION OF CERTAIN DISCLOSURE.—No communications common carrier or service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.

(d) DISSEMINATION BY BUREAU.—The Federal Bureau of Investigation may disseminate information and records obtained under this section only as provided in guidelines approved by the Attorney General for foreign intelligence collection and foreign counterintelligence investigations conducted by the Federal Bureau of Investigation, and, with respect to dissemination to an agency of the United States, only if such information is clearly relevant to the authorized responsibilities of such agency.

(e) REQUIREMENT THAT CERTAIN CONGRESSIONAL BODIES BE INFORMED.—On a semiannual basis the Director of the Federal Bureau of Investigation shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests made under subsection (b) of this section.

§ 2710. Definitions for chapter

As used in this chapter—

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

(2) the term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system.

PART II—CRIMINAL PROCEDURE

CHAPTER 205—SEARCHES AND SEIZURES

§ 3117. Mobile tracking devices

(a) IN GENERAL.—If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction.

(b) DEFINITION.—As used in this section, the term "tracking device" means an electronic or mechanical device which permits the tracking of the movement of a person or object.

CHAPTER 206—PEN REGISTERS

§ 3121. General prohibition on pen register use; exception

(a) IN GENERAL.—Except as provided in this section, no person may install or use a pen register without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(b) EXCEPTION.—The prohibition of subsection (a) does not apply with respect to the use of a pen register by a provider of electronic or wire communication service—

(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service, or with the consent or the user of that service.

(c) PENALTY.—Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

§ 3122. Application for an order for a pen register

(a) APPLICATION.—(1) An attorney for the Government may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction.

(2) Unless prohibited by State law, a State investigative or law enforcement officer may make application for an order or an extension of an order under section 3123 of this title authorizing or approving the installation and use of a pen register under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction of such State.

(b) CONTENTS OF APPLICATION.—An application under subsection (a) of this section shall include—

(1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and

(2) a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

§ 3123. Issuance of an order for a pen register

(a) IN GENERAL.—Upon an application made under section 3122 of this title, the court shall enter an ex parte order authorizing the installation and use of a pen register within the jurisdiction of the court if the court finds that the attorney for the Government or the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

(b) CONTENTS OF ORDER.—An order issued under this section—

(1) shall specify—

(A) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line to which the pen register is to be attached;

(B) the identity, if known, of the person who is the subject of the criminal investigation;

(C) the number and, if known, physical location of the telephone line to which the pen register is to be attached; and

(D) a statement of the offense to which the information likely to be obtained by the pen register relates; and

(2) shall direct, upon the request of the applicant, the furnishing of information, facilities, and technical assistance necessary to accomplish the installation of the pen register under section 3124 of this title.

(c) TIME PERIOD AND EXTENSIONS.—(1) An order issued under this section shall authorize the installation and use of a pen register for a period not to exceed 60 days.

(2) Extensions of such an order may be granted, but only upon an application for an order under section 3122 of this title and upon

the judicial finding required by subsection (a) of this section. The period of extension shall be for a period not to exceed 60 days.

(d) NONDISCLOSURE OF EXISTENCE OF PEN REGISTER.—An order authorizing or approving the installation and use of a pen register shall direct that—

(1) the order be sealed until otherwise ordered by the court; and

(2) the person owning or leasing the line to which the pen register is attached, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

§ 3124. Assistance in installation and use of a pen register

(a) IN GENERAL.—Upon the request of an attorney for the government or an officer of a law enforcement agency authorized to install and use a pen register under this chapter, a provider of wire communication service, landlord, custodian, or other person shall furnish such investigative or law enforcement officer forthwith all information, facilities, and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if such assistance is directed by a court order as provided in section 3123(b)(2) of this title.

(b) COMPENSATION.—A provider of wire communication service, landlord, custodian, or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

§ 3125. Reports concerning pen registers

The Attorney General shall annually report to Congress on the number of pen register orders applied for by law enforcement agencies of the Department of Justice.

§ 3126. Definitions for chapter

As used in this chapter—

(1) the term "communications common carrier" has the meaning set forth for the term "common carrier" in section 3(h) of the Communications Act of 1934 (47 U.S.C. 153(h));

(2) the term "wire communication" has the meaning set forth for such term in section 2510 of this title;

(3) the term "court of competent jurisdiction" means—

(A) a district court of the United States (including a magistrate of such a court) or a United States Court of Appeals; or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register;

(4) the term "pen register" means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted, with respect to wire communi-

cations, on the telephone line to which such device is attached, but such term does not include any device used by a provider of wire communication service for billing, or recording as an incident to billing, for communications services provided by such provider; and

(5) the term "attorney for the Government" has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and

(6) the term "State" means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.

* * * * * * *

O