example, online retailers need to disclose consumers' names and home addresses to shippers in order to fulfill customers' orders. This disclosure is obvious from the context of the consumer-retailer relationship. Retailers do not need to provide prominent notice of the practice (though they should disclose it in their full privacy notices); companies may infer that consumers have agreed to the disclosure based on the consumers' actions in placing the order and a widespread understanding of the product delivery process.

Several categories of data practices are both common to many contexts and integral to companies' operations. The example above falls into the more general category of product and service fulfillment; companies may infer consent to use and disclose personal data to achieve objectives that consumers have specifically requested, as long as there is a common understanding of the service. Similarly, companies may infer consent to use personal data to conduct marketing in the context of most first-party relationships, given the familiarity of this activity in digital and in-person commerce, the visibility of this kind of marketing, the presence of an easily identifiable party to contact to provide feedback, and consumers' opportunity to end their relationship with a company if they are dissatisfied with it. In addition, companies collect and use personal data for purposes that are common, even if they may not be well known to consumers. For example, analyzing how consumers use a service in order to improve it, preventing fraud, complying with law enforcement orders and other legal obligations, and protecting intellectual property all have been basic elements of doing business and meeting companies' legal obligations.[22] Companies should be able to infer consumer consent to collect personal data for these limited purposes, consistent with the other principles in the Consumer Privacy Bill of Rights.

In other cases, context should guide decisions about which opportunities for consumer control are reasonable for companies to provide and also meaningful to consumers. Information and choices that are meaningful to consumers in one context may be largely irrelevant in others. For example, consider a hypothetical game application for a mobile device that allows consumers to save the game's state, so that they can resume playing after a break. The hypothetical company that provides this game collects the unique identifier of each user's mobile device in order to provide this "save" function. Collecting the mobile device's unique identifier for this purpose may be consistent with the "save" function and consumers' decisions to use it, particularly if the company uses identifiers only for this purpose. If the company provides consumers' unique device identifiers to third parties for purposes such as online behavioral advertising, however, the company should notify consumers and allow them to prevent the disclosure of personal data.

The sophistication of a company's consumers is also a critical element of context. In particular, the privacy framework may require a different degree of protection for children's and teenagers' privacy interests from the protections afforded to adults due to the unique characteristics of these age groups. Children may be particularly susceptible to privacy harms. Currently, the Children's Online Privacy Protection Act (COPPA) and the FTC's implementing regulations provide strong protections by requiring online

22. This list of practices that are common to many contexts is similar to the "commonly accepted practices" that FTC staff identified in its 2010 report. *See* FTC Staff Report at 53-54. In the Administration's view, protecting intellectual property is so widespread and necessary to many companies that they should be able to infer consent to achieve this objective. Several commenters on the Department of Commerce's Privacy and Information Green Paper encouraged the Administration to recognize such practices in order to provide certainty for companies and to give greater prominence to choices that consumers are more likely to find meaningful.

services that are directed to children, or that know that they are collecting personal data from children, to obtain verifiable parental consent before they collect such data.[23] Online services that are "directed to" children must meet this same standard. The Administration looks forward to exploring with stakeholders whether more stringent applications of the Consumer Privacy Bill of Rights—such as an agreement not to create individual profiles about children, even if online services obtain the necessary consent to collect personal data—are appropriate to protect children's privacy.

The terms governing a company-to-consumer relationship are another key element of context. In particular, advertising supports innovative new services and helps to provide consumers with free access to a broad array of online services and applications. The Respect for Context principle does not foreclose any particular ad-based business models. Rather, the Respect for Context principle requires companies to recognize that different business models based on different personal data raise different privacy risks. A company should clearly inform consumers of what they are getting in exchange for the personal data they provide. The Administration also encourages companies engaged in online advertising to refrain from collecting, using, or disclosing personal data that may be used to make decisions regarding employment, credit, and insurance eligibility or similar matters that may have significant adverse consequences to consumers. Collecting data for such sensitive uses is at odds with the contextually well-defined purposes of generating revenue and providing consumers with ads that they are more likely to find relevant. Such practices also may be at odds with the norm of responsible data stewardship that the Respect for Context principle encourages.

Consider, for example, an online social networking service whose users disclose biographical information when creating an account and provide information about their social contacts and interests by including friends, business associates, and companies in their networks. As consumers use the service, they may generate large amounts of information that is associated with their identity on the online social network, including written updates, photos, videos, and location information. Consumers make affirmative choices to share this information with members of their online social networks. These disclosures are all integral to the company providing its social networking service. Furthermore, it is reasonable for the company to reveal at least some of these details to other members in order to help them form new connections.

Whether the online social networking service provider will use this information, and for what purposes, may be less clear from the context that consumers experience. The personal data that consumers generate may be valuable for improving the service, selling online advertising, or assembling individual profiles that the company provides to third parties. These uses fall along a continuum that starts at the core context of consumers engaging online with a group of associates. Consumers expect the company to improve its services. The company does not need to seek affirmative consent each time it uses existing data to improve a service, or even creates a new service, provided that these new uses of personal data are consistent with what users come to expect in a social networking context.

Suppose that the company leases individual profile information to third parties, such as information brokers. Respect for Context may not require the company to specify each use that a recipient might

23. *See* Children's Online Privacy Protection Act, Pub. L. 105-277 (codified at 15 U.S.C. §§ 6501-6506) *and* FTC, Children's Online Protection Rule, 16 C.F.R. Part 312. COPPA defines "child" to mean "an individual under the age of 13." 15 U.S.C. § 6501(1).

make of this data, but, at a minimum, it may require the company to state prominently and explicitly that it discloses personal data to third parties who may further aggregate and use this data for other purposes. The Respect for Context principle, in combination with other principles in the Consumer Privacy Bill of Rights, also calls on the company to provide consumers with meaningful opportunities to prevent these disclosures.

4. **SECURITY: Consumers have a right to secure and responsible handling of personal data.** Companies should assess the privacy and security risks associated with their personal data practices and maintain reasonable safeguards to control risks such as loss; unauthorized access, use, destruction, or modification; and improper disclosure.

Technologies and procedures that keep personal data secure are essential to protecting consumer privacy. Security failures involving personal data, whether resulting from accidents or deliberate attacks, can cause harms that range from embarrassment to financial loss and physical harm. Companies that lose control of personal data may suffer reputational harm as well as financial losses if business partners or consumers end their relationships after a security breach. These consequences provide companies with significant incentives to keep personal data secure. The security precautions that are appropriate for a given company will depend on its lines of business, the kinds of personal data it collects, the likelihood of harm to consumers, and many other factors.

The Security principle recognizes these needs. It gives companies the discretion to choose technologies and procedures that best fit the scale and scope of the personal data that they maintain, subject to their obligations under any applicable data security statutes, including their duties to notify consumers and law enforcement agencies if the security of data about them is breached, and their commitments to adopt reasonable security practices.

5. **ACCESS AND ACCURACY: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.** Companies should use reasonable measures to ensure they maintain accurate personal data. Companies also should provide consumers with reasonable access to personal data that they collect or maintain about them, as well as the appropriate means and opportunity to correct inaccurate data or request its deletion or use limitation. Companies that handle personal data should construe this principle in a manner consistent with freedom of expression and freedom of the press. In determining what measures they may use to maintain accuracy and to provide access, correction, deletion, or suppression capabilities to consumers, companies may also consider the scale, scope, and sensitivity of the personal data that they collect or maintain and the likelihood that its use may expose consumers to financial, physical, or other material harm.

An increasingly diverse array of entities uses personal data to make decisions that affect consumers in ways ranging from the ads they see online to their candidacy for employment. Outside of sectors covered by specific Federal privacy laws, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Fair Credit Reporting Act, consumers do not currently have the right to access and correct this data. The Administration is committed to publishing data on the Internet in machine-readable formats to advance the goals of innovation, transparency, participation, and collaboration. For example, to promote innovation and efficiency in the delivery of electricity, the Administration supports providing consumers with timely access to energy usage data in standardized, machine-readable formats over the Internet.[24] Similarly, the expanded use of health IT, including patients' access to health data through electronic health records, is a key element of the Administration's innovation strategy.[25] Comprehensive privacy and security safeguards, tailored for both contexts, are fundamental to both strategies.

Providing consumers with access to information about them in usable formats holds similar promise in the commercial arena. To help consumers make more informed choices, the Administration encourages companies to make personal data available in useful formats to the properly authenticated individuals over the Internet.[26]

The Access and Accuracy principle recognizes that the use of inaccurate personal data may lead to a range of harms. The risk of these harms, in addition to the scale, scope, and sensitivity of personal data that a company retains, help to determine what kinds of access and correction facilities may be reasonable in a given context. As a result, this principle does not distinguish between companies that are consumer-facing and those that are not. In all cases, however, the mechanisms that companies use to provide consumers with access to data about them should not create additional privacy or security risks.

United States Constitutional law has long recognized that privacy interests co-exist alongside fundamental First Amendment rights to freedom of speech, freedom of the press, and freedom of association. Individuals and members of the press exercising their free speech rights may well speak about other individuals and include personal information in their speech. The Access and Accuracy principle should therefore be interpreted with full respect for First Amendment values, especially for non-commercial speakers and individuals exercising freedom of the press.

---

24. National Science and Technology Council, *A Policy Framework for the 21st Century Grid: Enabling Our Secure Energy Future*, at 41, 46, June 2011, *available* at http://www.whitehouse.gov/sites/default/files/microsites/ostp/nstc-smart-grid-june2011.pdf.

25. See The White House, *A Strategy for American Innovation: A Strategy for American Innovation: Securing Our Economic Growth and Prosperity*, Feb. 2011, http://www.whitehouse.gov/innovation/strategy; Department of Health and Human Services, Final Rule on Electronic Health Record Incentive Program, 75 Fed. Reg. 44314, July 28, 2010.

26. *See* Memorandum for the Heads of Executive Departments and Agencies, "Informing Consumers Through Smart Disclosure," *available at* http://www.whitehouse.gov/sites/default/files/omb/inforeg/for-agencies/informing-consumers-through-smart-disclosure.pdf ("To the extent practicable and subject to valid restrictions, agencies should publish information online in an open format that can be retrieved, downloaded, indexed, and searched by commonly used Web search applications. An open format is one that is platform independent, machine readable, and made available to the public without restriction that would impede the re-use of that information."); M-10-06, Memorandum for the Heads of Executive Departments and Agencies, "Open Government Directive," *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-06.pdf ("Machine readable data are digital information stored in a format enabling the information to be processed and analyzed by computer. These formats allow electronic data to be as usable as possible.").

6. **FOCUSED COLLECTION: Consumers have a right to reasonable limits on the personal data that companies collect and retain.** Companies should collect only as much personal data as they need to accomplish purposes specified under the Respect for Context principle. Companies should securely dispose of or de-identify personal data once they no longer need it, unless they are under a legal obligation to do otherwise.

The Focused Collection principle holds that companies should engage in considered decisions about the kinds of data they need to collect to accomplish specific purposes. For example, the hypothetical game company referenced above that collects the unique identifier of each user's mobile device in order to provide a "save" function should consider whether it must use the mobile device identifier or whether a less broadly linkable identifier would work as well. Nevertheless, as discussed under the Respect for Context principle, companies may find new uses for personal data after they collect it, provided they take appropriate measures of transparency and individual choice. The Focused Collection principle does not relieve companies of any independent legal obligations, including law enforcement orders, that require them to retain personal data.

Wide-ranging data collection may be essential for some familiar and socially beneficial Internet services and applications. Search engines are one example. Search engines gather detailed data about the contents and structure of the World Wide Web. Consumers understand and depend on search engines to collect this broad range of data and make it available for a wide range of end uses. Search engines also log search queries to improve their services. Search engines may collect such data, which includes personal data, in a manner that is consistent with the Focused Collection principle, so long as their purposes for collecting personal data are clear, and they do not retain personal data beyond the time they need it to achieve any of these purposes.

7. **ACCOUNTABILITY: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.** Companies should be accountable to enforcement authorities and consumers for adhering to these principles. Companies also should hold employees responsible for adhering to these principles. To achieve this end, companies should train their employees as appropriate to handle personal data consistently with these principles and regularly evaluate their performance in this regard. Where appropriate, companies should conduct full audits. Companies that disclose personal data to third parties should at a minimum ensure that the recipients are under enforceable contractual obligations to adhere to these principles, unless they are required by law to do otherwise.

Privacy protection depends on companies being accountable to consumers as well as to agencies that enforce consumer data privacy protections. The Accountability principle, however, goes beyond external accountability to encompass practices through which companies prevent lapses in their privacy commitments or detect and remedy any lapses that may occur. Companies that can demonstrate that they live up to their privacy commitments have powerful means of maintaining and strengthening consumer trust. A company's own evaluation can prove invaluable to this process. The appropriate evaluation technique, which could be a self-assessment and need not necessarily be a full audit, will depend on the size, complexity, and nature of a company's business, as well as the sensitivity of the data involved. In recent years, chief privacy officers—experts who raise awareness of privacy issues in companies that face rapid changes in technologies, consumer expectations, and regulations—have emerged as a valuable source of guidance and internal evaluation. Chief privacy officers are likely to provide a continuing source of guidance within companies throughout the development of products and services.

To be fully effective, however, companies should link evaluations to the enforcement of pre-established internal expectations; evaluations are not an end in themselves. Audits—whether conducted by the company or by an independent third party—may be appropriate under some circumstances, but they are not always necessary to fulfill the Accountability principle.

Moreover, accountability must attach to data transferred from one company to another. From the perspective of the Consumer Privacy Bill of Rights, the emphasis is not on the disclosures themselves, but on whether a disclosure leads to a use of personal data that is inconsistent within the context of its collection or a consumer's expressed desire to control the data. Thus, if a company transfers personal data to a third party, it remains accountable and thus should hold the recipient accountable—through contracts or other legally enforceable instruments—for using and disclosing the data in ways that are consistent with the Consumer Privacy Bill of Rights.

III. Implementing the Consumer Privacy Bill of Rights: Multistakeholder Processes to Develop Enforceable Codes of Conduct

Implementing the general principles in the Consumer Privacy Bill of Rights across the wide range of innovative uses of personal data requires a process to establish more specific practices. The Administration encourages individual companies, industry groups, privacy advocates, consumer groups, crime victims, academics, international partners, State Attorneys General, Federal civil and criminal law enforcement representatives, and other relevant groups to participate in multistakeholder processes to develop codes of conduct that implement these general principles.

In consumer data privacy, as in other areas affecting Internet policy, the Administration believes that multistakeholder processes underlie many of the institutions responsible for the Internet's success. This reflects the Administration's abiding commitment to preserving the Internet as anopen, decentralized, user-driven platform for communication, innovation, and economic growth.[27]

The Administration supports open, transparent multistakeholder processes because, when appropriately structured, they can provide the flexibility, speed, and decentralization necessary to address Internet policy challenges. A process that is open to a broad range of participants and facilitates their full participation will allow technical experts, companies, advocates, civil and criminal law enforcement representatives responsible for enforcing consumer privacy laws, and academics to work together to find creative solutions to problems. Flexibility in the deliberative process is critical to allowing stakeholders to explore the technical and policy dimensions—which are often intertwined—of Internet policy issues. Moreover, the United States will need to confront a broad, complex, and global set of consumer data privacy issues for decades to come. A process that works efficiently and on a global scale is therefore essential.

Another key advantage of multistakeholder processes is that they can produce solutions in a more timely fashion than regulatory processes and treaty-based organizations. In the Internet standards world, for example, working groups frequently form around a specific problem and make significant progress toward a solution within months, rather than years. These groups frequently function on the basis of consensus and are amenable to the participation of individuals and groups with limited resources. These characteristics lend legitimacy to the groups and their solutions, which in turn can encourage rapid and effective implementation.

---

27. The United States recently joined the other members of the Organisation for Economic Co-operation and Development (OECD) in recognizing the economic and social importance of the Internet. *See* OECD, Communiqué on Principles for Internet Policy-Making, OECD High-Level Meeting on The Internet Economy: Generating Innovation and Growth, June 28-29, 2011, http://www.ntia.doc.gov/legacy/ntiahome/privwhitepaper.html.

Finally, multistakeholder processes do not rely on a single, centralized authority to solve problems. Specific multistakeholder institutions address specific kinds of Internet policy challenges. This kind of specialization not only speeds up the development of solutions but also helps to avoid the duplication of stakeholders' efforts.

Due in part to its reliance on multistakeholder processes, United States Internet policy has generally avoided fragmented, prescriptive, and unpredictable rules that frustrate innovation and undermine consumer trust. The United States has also refrained from adopting legal requirements that prescribe specific technical requirements, which could fragment the global market for information technologies and services and inhibit innovation. Instead, the United States generally defers to the expert bodies that produce Internet technical standards. In addition, the Administration continues its support for Internet policy processes that are open, transparent, and promote cooperation within a legal framework that sets appropriate performance requirements for individuals and companies.

Consumer data privacy issues exemplify the need for multistakeholder processes that develop the practices and technologies necessary to implement general policy principles. Experience in the United States has shown that both companies and consumers benefit when companies commit to the task of innovating privacy practices. In the early days of commercial activity on the Internet (mid-1990s to early 2000s), for example, the Department of Commerce, the FTC, and the White House convened stakeholders to gather information about privacy issues in this rapidly evolving marketplace. These efforts yielded a flexible, voluntary privacy framework that provided meaningful privacy protections while fostering dynamic innovations in technologies and business models.[28]

Even without legislation, the Administration intends to convene and facilitate multistakeholder processes to produce enforceable codes of conduct. In an open forum, stakeholders with an interest in a specific market or business context will work toward consensus on a legally enforceable code of conduct that implements the Consumer Privacy Bill of Rights. Multistakeholder processes are different from traditional agency rulemakings. The Federal Government will work with stakeholders to establish operating procedures for an open, transparent process. Ultimately, however, the stakeholders themselves will control the process and its results. There is no Federal regulation at the end of the process, and codes will not bind any companies unless they choose to adopt them.

The incentive for stakeholders to participate in this process is twofold. Companies will build consumer trust by engaging directly with consumers and other stakeholders during the process. Adopting a code of conduct that stakeholders develop through this process would further build consumer trust. Second, in any enforcement action based on conduct covered by a code, the FTC will consider a company's adherence to a code favorably.

---

28. For example, the combined efforts of the Department of Commerce, FTC, and the White House produced the consumer data privacy framework of notice and choice, which protected privacy in the context of rapidly developing technologies and markets. *See* FTC, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress, at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (2000); White House, *Framework for Global Electronic Commerce, at* § 5, http://clinton4.nara.gov/WH/New/Commerce/ (1997); National Telecommunications and Information Administration, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information* (Oct. 1995), http://www.ntia.doc.gov/legacy/ntiahome/privwhitepaper.html.

A. Building on the Successes of Internet Policymaking

The Internet provides several successful examples of the kind of multistakeholder policy development the Administration envisions. Private-sector standards-setting organizations, for example, are at the forefront of setting Internet-related technical standards. Groups such as the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C) use transparent processes to set Internet-related technical standards. These processes are successful, in part, because stakeholders share an interest in developing consensus-based solutions to the underlying challenges. The success of the resulting standards is evident in the constantly growing range of services and applications—as well as the trillions of dollars in global commerce—they support.

Similarly, the Internet Corporation for Assigned Names and Numbers (ICANN), a nonprofit corporation, coordinates the technical management of the domain name system, which maps domain names to unique numerical addresses. ICANN is also a multistakeholder organization that includes representatives from a broad array of interests, including generic top level domain registries, registrars and registrants, country code top level domain registries, the Regional Internet Registries, root server operators, national governments, and Internet users at large. With this structure, ICANN coordinates the technical management of an important function of the Internet—mapping names that people can remember to numerical addresses that computers can use—and does so in a manner that allows for a wide range of stakeholder input.

Government-convened policymaking efforts, such as the Executive Branch-led privacy discussions of the 1990s and early 2000s, continue to be central to advancing consumer data privacy protections in the United States. The framework in this document is a direct result of the Department of Commerce Internet Policy Task Force's extensive engagement with stakeholders—companies, trade groups, privacy advocates, academics, civil and criminal law enforcement representatives, and foreign government officials. In addition, the FTC has encouraged multistakeholder efforts to develop a "Do Not Track" mechanism, which would afford greater consumer control over personal data in the context of online behavioral advertising.

B. Defining the Multistakeholder Process for Consumer Data Privacy

The Department of Commerce's National Telecommunications and Information Administration (NTIA) has the necessary authority and expertise, developed through its role in other areas of Internet policy, to convene multistakeholder processes that address consumer data privacy issues.[29] NTIA will lead the Department of Commerce's convening of stakeholders in a deliberative process that develops codes of conduct and allows stakeholders to adapt the codes to protect consumers' privacy as technologies and market conditions change.[30]

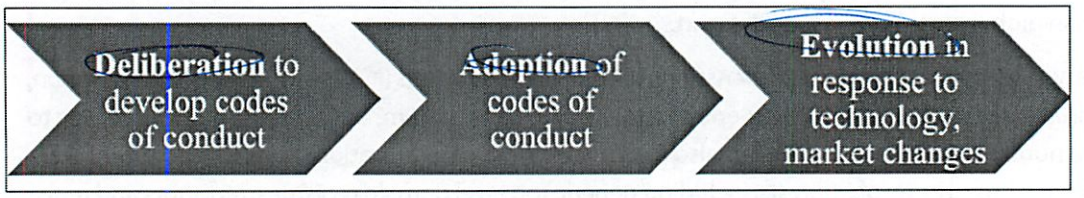


Figure 1. The principal stages of the multistakeholder process for consumer data privacy

1. *Deliberation*

- **Identifying Issues.** Stakeholder groups, with the assistance of NTIA, will identify markets and industry sectors that involve significant consumer data privacy issues and may be ripe for an enforceable code of conduct. The process will be open, but the focus of a given process likely will not appeal equally to all stakeholders.
- **Initiating and Facilitating Deliberations.** NTIA will take steps to enlist the participation of stakeholders to develop an enforceable code of conduct. As convener, NTIA will open meetings to all stakeholders, including international partners, the FTC, Federal civil and criminal law enforcement representatives, and State Attorneys General, that have an interest in defining an appropriate code of conduct and express a willingness to work in good faith toward reaching consensus on the code's provisions.

  As their first order of business, stakeholders will establish operating processes and procedures. The Administration is committed to a process that is open, transparent, and accommodates participation by groups that have limited resources; however the deliberative process must meet the needs of its participants, who determine and abide by its outcome.[31]

29. NTIA is designated by statute as the "President's principal adviser on telecommunications policies pertaining to the Nation's economic and technological advancement . . . ." 47 U.S.C. § 902(b)(2)(D).

30. Other Federal agencies may play this convening role if consumer data privacy issues arise in their areas of expertise. Alternatively, private-sector organizations could convene stakeholders, though the dearth of private sector-led code development efforts is precisely the reason that the Administration proposes to serve as convener.

31. The Administration's guidelines for increasing transparency, participation, and collaboration in public policy development could prove useful here. See President Barack Obama, Memorandum to the Heads of Executive Departments and Agencies: Transparency and Open Government, http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment/; Peter R. Orszag, Memorandum for the Heads of Executive Departments and Agencies: Open Government Directive, Dec. 8, 2009, http://www.whitehouse.gov/open/documents/open-government-directive.

- **Conclusion.** A code that reflects the agreement of all stakeholders is ready for companies to consider adopting. The Administration expects, however, that consensus will emerge on parts of a code, and that stakeholders are likely to resolve the most difficult issues later in the process. At this stage, NTIA may need to work intensively with stakeholders to help them resolve their differences. NTIA's role will be to help the parties reach clarity on what their positions are and whether there are options for compromise toward consensus, rather than substituting its own judgment. To minimize the possibility that some stakeholders may draw inflexible lines that prevent consensus, the parties should discuss and set out rules or procedures at the outset of the process to govern how the group will reach an orderly conclusion, even if there is not complete agreement on results.

2. *Adoption*

Once a code of conduct is complete, companies to which the code is relevant may choose to adopt it. The Administration expects that a company's public commitment to adhere to a code of conduct will become enforceable under Section 5 of the FTC Act (15 U.S.C. § 45), just as a company is bound today to follow its privacy statements.[32] Enforceability is essential to assuring consumers that companies' practices match their commitments and thus to strengthening consumer trust.

3. *Evolution*

A key goal of the multistakeholder process is to enable stakeholders to modify privacy protections in response to rapid changes in technology, consumer expectations, and market conditions, to assure they sufficiently protect consumer data privacy. The multistakeholder process offers several ways to keep codes of conduct current. Stakeholders may decide at any time that a code of conduct no longer provides effective consumer data privacy protections, in light of technological or market changes. NTIA might also draw this conclusion and seek to re-convene stakeholders. As with the initial development of a code of conduct, however, stakeholder participation in the process to revise a code of conduct would be voluntary. The Federal Government would not revise a code of conduct; rather, stakeholder groups will make these changes with Federal Government input. Finally, under the legislative safe harbor framework discussed in the following section, Congress could prescribe a renewal period for codes of conduct, so that the FTC periodically reviews codes that are the basis of enforcement safe harbors.

32. The FTC brings cases based on violations of commitments in its privacy statements under its authority to prevent deceptive acts or practices. In addition, the FTC brings data privacy cases under its unfairness jurisdiction, which will remain an important source of consumer data privacy protection.

IV. Building on the FTC's Enforcement Expertise

A. Protecting Consumers Through Strong Enforcement

Enforcement is critical to ensuring that the privacy commitments companies make by adopting a code of conduct are meaningful. Self-regulatory bodies, which develop and administer voluntary guidelines for member companies, can provide a first line of enforcement, though they are not necessary for the framework described here. Enforcement through self-regulatory bodies can help to detect and remedy compliance issues at an early stage. As a result, this kind of enforcement can strengthen trust in a code of conduct and the companies that commit to the code.

Government agencies also play a vital role in enforcing the privacy protections in codes of conduct. The FTC is the Federal Government's leading consumer privacy enforcement authority.[33] Enforcement actions by the FTC (and State Attorneys General) have established that companies' failures to adhere to voluntary privacy commitments, such as those stated in privacy policies, are actionable under the FTC Act's (and State analogues) prohibition on unfair or deceptive acts or practices.[34] In addition, the FTC brings cases against companies that allegedly failed to use reasonable security measures to protect personal information about consumers.[35] Using this authority, the FTC has brought cases that effectively protect consumer data privacy within a flexible and evolving approach to changing technologies and markets. The same authority would allow the FTC to enforce the commitments of companies under its jurisdiction to adhere to codes of conduct developed through the multistakeholder process.[36] Thus, companies that adopt codes of conduct will make commitments that are legally enforceable under existing law.

B. Providing Incentives to Develop Enforceable Codes of Conduct

The FTC has significant enforcement and policy expertise to offer all stakeholders on consumer data privacy issues codes of conduct. With or without consumer data privacy legislation, the FTC should provide assistance and advice regarding development of the codes. In the absence of legislation, the FTC, Federal civil and criminal law enforcement representatives, and States should participate in the multistakeholder deliberations by providing advice on substance and process. Once stakeholders have developed a code, a company may voluntarily adhere to the code in order to gain greater certainty and

33. Note, however, the FTC does not currently have authority to enforce Section 5 of the FTC Act, 15, U.S.C. § 45, against certain corporations that operate for profit.

34. *See* FTC Act § 5, 15 U.S.C. § 45. In addition to using its Section 5 authority to protect consumer data privacy, the FTC has brought dozens of cases under sector-specific statutes, such as the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, and the Do Not Call Rule. For a review of these cases, see FTC Staff Report at 9-13.

35. *See* FTC Staff Report at 10 (reviewing enforcement actions that include counts based on unfair acts or practices).

36. The FTC's jurisdiction over nonprofits and certain other types of entities under FTC Act § 5 may be limited.

assure its customers that its practices protect their privacy. Companies may choose to adopt multiple codes of conduct to cover different lines of business; the common baseline of the Consumer Privacy Bill of Rights should help ensure that the codes are consistent. Then, in any investigation or enforcement action related to the subject matter of one or more codes, the FTC should consider the company's adherence to the codes favorably.

V. Promoting International Interoperability

The Internet helps U.S. companies expand across borders. As a result, cross-border data flows are a vital component of the domestic and global economies. Differences in national privacy laws create challenges for companies wishing to transfer personal data across national borders. Complying with different privacy laws is burdensome for companies that transfer personal data as part of well-defined, discrete data processing operations because legal standards may vary among jurisdictions, and companies may need to obtain multiple regulatory approvals to conduct even routine operations.

Services that cater to individual users face steeper compliance challenges because they handle data flows that are more complex and varied. Further complicating matters is the proliferation of cloud computing systems.[37] This globally distributed architecture helps deliver cost-effective, innovative new services to consumers, companies, and governments. It also allows consumers and companies to send the personal data they generate and use to recipients all over the world. Consumer data privacy frameworks should not only facilitate these technologies and business models but also adapt rapidly to those that have yet to emerge.

Though governments may take different approaches to meeting these challenges, it is critical to the continued growth of the digital economy that they strive to create interoperability between privacy regimes. The Administration believes flexible multistakeholder processes that address novel uses and transfers of data facilitate interoperable privacy regimes. The United States is committed to engaging with its international partners to increase interoperability in privacy laws by pursuing mutual recognition, the development of codes of conduct through multistakeholder processes, and enforcement cooperation. It is also committed to including international counterparts in these multistakeholder processes, to enable global consensus on emerging privacy issues.

A. Mutual Recognition

Mutual recognition of commercial data privacy frameworks is a means to achieve meaningful global data protection. A starting point for mutual recognition is the embrace of common values surrounding privacy and personal data protection. Two principles should determine whether the conditions for mutual recognition between specific privacy frameworks exist: effective enforcement and mechanisms that allow companies to demonstrate accountability.

Where companies are under comparable legal requirements, mutual recognition means that all parties can enforce the companies' obligations. Effective enforcement, conducted according to publicly announced policies, is therefore critical to establishing interoperability. Enforcement authorities and mechanisms vary from country to country, and the United States recognizes that a variety of approaches can be effective. The United States relies primarily upon the FTC's case-by-case enforcement of general

37. NIST has identified five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. *See supra* note 6.

prohibitions on unfair or deceptive acts and practices. This approach helps develop evolving standards for handling personal data in the private sector.

In the context of mutual recognition, accountability refers to a company's capacity to demonstrate the implementation of enforceable policies and procedures relating to privacy (whether adopted voluntarily or as a result of legal obligations). Accountability mechanisms include self-assessments, evaluations, and audits.[38] The Administration encourages stakeholders to work together to identify globally accepted accountability mechanisms when developing codes of conduct.

One example of an initiative to facilitate transnational mutual recognition is the Asia-Pacific Economic Cooperation's (APEC) voluntary system of Cross Border Privacy Rules (CBPR), which is based on the APEC Privacy Framework and includes privacy principles that APEC member economies have agreed to recognize.[39] Codes of conduct based on these principles could streamline the data privacy policies and practices of companies operating throughout the vast APEC region.[40] Upon implementation, APEC's CBPR system will require interested applicants to demonstrate that they comply with a set of CBPR program requirements based on the APEC Privacy Framework. Moreover, the commitments an applicant makes during this process, while voluntary, must be enforceable under laws in member economies. Successful CBPR certification will entitle participating companies to represent to consumers that they are accountable and meet stringent and globally recognized standards, thereby facilitating the transfer of personal data throughout the APEC region.

In Europe, Article 27 of European Union (EU) Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, commonly known as the EU Data Protection Directive, encourages the development of codes of conduct to help implement the law. Like the Administration's framework, which proposes industry-specific codes of conduct, the Data Protection Directive recognizes that codes of conduct that implement general privacy principles may differ in their details, according to the needs of the relevant industry. The Administration is committed to working with organizations at the EU level as well as with member states to make codes of conduct the basis of mutually recognized privacy protections.

The Safe Harbor Frameworks that the United States developed with the EU and Switzerland are early examples of global interoperability that have had a meaningful impact on transatlantic data flows. The United States, the EU, and Switzerland negotiated these Frameworks to accomplish the objectives of protecting personal information while also ensuring that companies could transfer information in a way that did not disrupt their global business operations. These Frameworks allow companies to self-certify that they comply with requirements under the EU Data Protection Directive, subject to FTC

38. Auditing is not a requirement under the Accountability principle stated in the Consumer Privacy Bill of Rights. This section discusses the potential use of audits by companies that seek to take advantage of global interoperability in privacy laws. Not all organizations, however, fit this description.

39. The nine principles are collection limitation, integrity of personal information, notice, uses of personal information, choice, security safeguards, access and correction, accountability, and harm prevention. *See* http://publications.apec.org/publication-detail.php?pub_id=390.

40. Currently, APEC includes 21 members: Australia, Brunei Darussalam, Canada, Chile, the People's Republic of China, Hong Kong, Indonesia, Japan, the Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, the Philippines, Russia, Singapore, Chinese Taipei, Thailand, the United States, and Vietnam. APEC, Member Economies, http://www.apec.org/About-Us/About-APEC/Member-Economies.aspx (last visited Sept. 7, 2011).

enforcement of these representations.[41] The more than 2,700 companies that participate in the Safe Harbor Frameworks may transfer personal data from the EU to the United States. As a result, the Safe Harbor Frameworks have effectively reduced barriers to personal data flow and thereby support trade and economic growth.

B. An International Role for Multistakeholder Processes and Codes of Conduct

The attributes of speed, flexibility and decentralized problem-solving in well-structured multistakeholder consultations offer certain advantages over traditional government regulation when it comes to establishing globally applicable rules and guidelines that promote innovation and protect consumers. Multistakeholder-developed codes of conduct, combined with existing mutual recognition frameworks, hold the promise of greatly simplifying companies' compliance burdens.

While the Safe Harbor Frameworks have proven to be valuable in facilitating transatlantic trade, they are not perfect solutions for all U.S. entities. Sectors not regulated by the FTC, such as financial services, telecommunications common carriers, and insurance, are not covered by the Safe Harbor Frameworks. Some companies in these sectors have indicated that they would like to see an improved environment for transatlantic data transfers.

To build on the success of the Safe Harbor Frameworks, the Administration, through the Departments of Commerce and State, plans to develop additional mechanisms—such as jointly developed codes of conduct—that support mutual recognition of legal regimes, facilitate the free flow of information, and address emerging privacy challenges. The Administration hopes to include international stakeholders in the multistakeholder processes. The Safe Harbor Frameworks could one day be supplemented by codes of conduct reflecting transatlantic consensus on important, emerging privacy issues.

C. Enforcement Cooperation

To realize global interoperability in data protection, mutual recognition must be accompanied by robust enforcement cooperation. Such collaboration, whether bilateral or multilateral, is necessary to address information sharing among data protection authorities.

Empowered by legislation that grants it greater authority to cooperate with foreign counterparts, the FTC helped to create the Global Privacy Enforcement Network ("GPEN"). GPEN aims to further the development of privacy enforcement priorities, sharing of best practices, and support for joint enforcement initiatives. The FTC is involved in a number of other international organizations, including the OECD, APEC, the Asia-Pacific Privacy Authorities forum, and the International Conference of Data Protection and Privacy Commissioners. The work of the United States Government in GPEN, the OECD, APEC, and other venues is increasing collaboration in privacy investigations and enforcement actions globally. Given that Internet-based services reach individuals in jurisdictions around the world, it is neither effective nor wise policy for governments to enforce national data privacy legislation in isolation.

---

41. For a summary of the FTC's enforcement of the U.S.-EU Safe Harbor Framework, see FTC, FTC Settles with Six Companies Claiming to Comply with International Privacy Framework, Oct. 6, 2009, http://www.ftc.gov/opa/2009/10/safeharbor.shtm. *See also In re* Google, Inc., Complaint, at 7 File No. 102 3136, Mar. 30, 2011 (alleging "respondent did not adhere to the US Safe Harbor Privacy Principles of Notice and Choice").

VI. Enacting Consumer Data Privacy Legislation

The Administration urges Congress to pass legislation adopting the Consumer Privacy Bill of Rights. Legislation would promote trust in the digital economy by providing a basic set of privacy rights throughout areas of the commercial sector that are not currently subject to specific Federal data privacy legislation. The flexible approach that the Administration supports will allow companies to implement the Consumer Privacy Bill of Rights in ways that fit the context in which they do business.

A. Codify the Consumer Privacy Bill of Rights

Congress should act to protect consumers from violations of the rights defined in the Administration's proposed Consumer Privacy Bill of Rights. These rights provide clear protection for consumers and define rules of the road for the rapidly growing marketplace for personal data.[42] The legislation should permit the FTC and State Attorneys General to enforce these rights directly. The legislation will need to state companies' obligations under the Consumer Privacy Bill of Rights with greater specificity than this document provides. The Consumer Privacy Bill of Rights is a guide for the Administration to work collaboratively with Congress on statutory language.[43]

To provide greater legal certainty and to encourage the development and adoption of industry-specific codes of conduct, the Administration also supports legislation that authorizes the FTC to review codes of conduct and grant companies that commit to adhere—and do adhere—to such codes forbearance from enforcement of provisions of the legislation.

In addition, consumer data privacy legislation should avoid:

- Adding duplicative or overly burdensome regulatory requirements to companies that are already adhering to legislatively adopted privacy principles.
- Prescribing technology-specific means of complying with the law's obligations.
- Precluding new business models that are consistent with the Consumer Privacy Bill of Rights in general but may involve new uses of personal information not contemplated at the time the statute is written.
- Altering existing statutory or regulatory authorities pursuant to which the government may obtain information that is necessary to assist in conducting border searches, investigating criminal conduct or other violations of law, or protecting public safety and national security.

42. The Administration is separately considering the need to amend laws pertaining to the government's access to data in the possession of private parties, including the Electronic Communications Privacy Act, to address changes in technology.

43. In the absence of legislation, the Consumer Privacy Bill of Rights set forth in this document provides guidance for stakeholders and does not alter the FTC's existing enforcement authority under FTC Act § 5.

- Contravening the ability of law enforcement to investigate and prosecute criminal acts, and ensure public safety.
- Altering existing statutory, regulatory, or policy authorities that apply to the government's information practices or address privacy issues outside of a purely commercial, consumer-oriented context.

B. Grant the FTC Direct Enforcement Authority

The Administration encourages Congress to grant the FTC the authority to enforce each element of the statutory Consumer Privacy Bill of Rights.[44] This authority would provide greater certainty to consumers and companies both. Companies would begin with a clearer roadmap to their privacy obligations. Consumers would benefit from knowing that Congress has empowered the FTC to enforce a comprehensive set of privacy protections in the commercial marketplace. At the same time, a statute that allows the FTC to enforce the Consumer Privacy Bill of Rights directly would provide flexibility and permit the FTC to address emerging privacy issues through specific enforcement actions governed by applicable procedural safeguards. Companies seeking even greater certainty under such legislation should use the multistakeholder process and enforcement safe harbor discussed below to develop context-specific codes of conduct in a timely fashion. The Administration recommends that Congress grant the same authority to State Attorneys General. So long as they coordinate with the FTC in their enforcement actions, States could provide additional enforcement resources and a considerable source of consumer data privacy expertise.

In domains involving rapid changes in technology and business practices, Congress has chosen to create flexible standards rather than tailoring them to technologies and practices that exist at the time it passes a law. In the realm of antitrust, for example, the Sherman Act prohibits agreements "in restraint of trade."[45] The Copyright Act defines basic terms such as "copies," "devices," and "processes" with reference to technologies "now known or later developed."[46] And, in the realm of data privacy, the FTC has brought numerous enforcement actions under the FTC Act Section 5's prohibition on "unfair or deceptive acts or practices." A combination of agency guidelines, judicial interpretation, and industry practices provides interpretations of these terms to allow individuals and companies to determine with greater certainty whether their conduct complies with these general laws.

The Administration encourages Congress to follow a similar path with baseline consumer data privacy legislation. It is important that a baseline statute provide a level playing field for companies, a consistent set of expectations for consumers, and greater clarity and transparency in the basis for FTC enforcement actions. The FTC also could engage the public to clarify how it will enforce the statutory Consumer Privacy Bill of Rights. The primary mechanisms to clarify the statute's requirements should be the multistakeholder process and enforcement safe harbor, based on enforceable codes of conduct, as discussed below. The more traditional modes of clarifying general statutory requirements, however, could also play a helpful role.

---

44. The FTC refers civil penalty actions to the Department of Justice, which may bring an action within 45 days. If the Department of Justice declines to litigate, the FTC may prosecute the case itself. *See, e.g.*, 15 U.S.C. § 56(a).

45. 15 U.S.C § 1.

46. 17 U.S.C. § 101.

C. Provide Legal Certainty Through an Enforcement Safe Harbor

The Administration supports authorizing the FTC to provide greater assurance to companies that adopt enforceable codes of conduct than is possible under current law. Two legislative structures would help to accomplish this goal. First, the FTC should have explicit authority to review codes of conduct against the Consumer Privacy Bill of Rights, as they are set forth in legislation. Legislation should require the FTC to review codes submitted for review within a reasonable amount of time (e.g., 180 days), require the FTC to consider public comments on a code, limit its review authority to approving or rejecting a code that reflects the consensus of all participants in the multistakeholder process, and establish a period for reviewing approved codes to ensure that they sufficiently protect consumer privacy in light of technological and market changes. The record from the multistakeholder process that produced a code—and particularly the presence of general consensus on its provisions—would help to guide the FTC's assessment of whether a code sufficiently implements the Consumer Privacy Bill of Rights. Because the outcome of FTC review will likely influence companies' decisions to adopt codes of conduct—the end result of the multistakeholder process—it is appropriate to determine the details of FTC review through a process that is open to all stakeholders. These details, however, need to be legally binding. Accordingly, the Administration recommends that Congress grant the FTC authority under the Administrative Procedure Act (5 U.S.C. § 552 *et seq.*) to issue rules that establish a fair and transparent process for reviewing and approving codes of conduct.

The second element that the Administration recommends is giving the FTC the authority to grant a "safe harbor"—that is, forbearance from enforcement of the statutory Consumer Privacy Bill of Rights—to companies that follow a code of conduct that the FTC has reviewed and approved. Companies that decline to adopt a code of conduct, or choose not to seek FTC review of a code that they do adopt, would simply be subject to the general obligations of the legislatively adopted Consumer Privacy Bill of Rights.

D. Balance Federal and State Roles in Consumer Data Privacy Protection

Federal legislation that enacts a Consumer Privacy Bill of Rights should provide a national standard for protecting consumer data privacy where existing Federal data privacy statutes do not apply. Nationally uniform consumer data privacy rules are necessary to create certainty for companies and consistent protections for consumers. These rules should take into consideration the need for certain information to be available for law enforcement-related purposes. Moreover, national uniformity is crucial to preserving the incentives that the Administration's framework provides through the multistakeholder process. Stakeholders' incentives to participate in the multistakeholder process, and companies' incentives to adopt codes of conduct, would be diminished if States enacted laws with more stringent requirements. The Administration therefore recommends that Congress preempt State laws to the extent they are inconsistent with the Consumer Privacy Bill of Rights as enacted and applied. The Administration also recommends that Congress provide forbearance from enforcement of State laws against companies that adopt and comply with FTC-approved codes of conduct.

The Administration's proposed approach preserves important policymaking and enforcement roles for the States. States can and should play a highly constructive role in the multistakeholder process. The Administration also supports granting State Attorneys General with the authority to enforce the

Consumer Privacy Bill of Rights. Taken together, these mechanisms will provide States means to address consumer data privacy issues that States identify while maintaining uniformity at the national level. The Administration will also work with Congress, States, the private sector, and other stakeholders to determine whether there are specific sectors in which States could enact laws that would not disrupt the broader uniformity the Administration seeks in consumer data privacy protections. For example, it may be appropriate to allow States to enact laws that apply the Consumer Privacy Bill of Rights to personal data in sectors they closely regulate, such as retail electricity distribution.[47]

E. Preserve Effective Protections in Existing Federal Data Privacy Laws

Consumer data privacy legislation should preserve existing sector-specific Federal laws that effectively protect personal data, minimize the duplication of legal requirements, and provide consumers with a clear sense of what protections they have and who enforces them. Where existing Federal laws do not meet these guidelines, however, the Administration encourages Congress to consider how consumer data privacy legislation could simplify existing requirements, to the benefit of consumers and companies.

In general, the sector-specific Federal data privacy laws establish legal obligations that are tailored to the sensitivity of personal data used and the prevailing practices in those sectors.[48] For instance, HIPAA and the HIPAA Privacy and Security Rules regulate the collection, use, and disclosure of personal health information by healthcare providers, insurers, and health information clearinghouses. HIPAA permits by default personal health information practices that are necessary or commonly accepted in the healthcare context, such as disclosures of personal health information between two healthcare providers in order to treat a patient. Federal data privacy laws that apply to education, credit reporting, financial services, and the collection of children's personal data are examples of similarly well-tailored requirements.

1. Create Comprehensive Privacy Protection Without Duplicating Burdens

To avoid creating duplicative regulatory burdens, the Administration supports exempting companies from consumer data privacy legislation to the extent that their activities are subject to existing Federal data privacy laws. However, activities within such companies that do not fall under an existing data privacy law would be covered by the legislation that the Administration proposes. The alternative—exempting entire entities that are subject to an existing Federal data privacy law—could allow the exception to swallow the rule. For example, the Gramm-Leach-Bliley Act (GLB) requires financial institutions to take certain privacy and security precautions with nonpublic personal information. If entities that are subject to GLB were exempt from a baseline consumer data privacy law for non-GLB-covered personal data, the baseline statute's effectiveness could be significantly diminished.

47. Indeed, the Administration recently called for State public utilities commissions to follow privacy principles that are very similar to those in the Consumer Privacy Bill of Rights in order to protect personal data associated with the "smart" electric grid. *See supra* note 23.

48. This limitation also means that the laws that regulate the Federal government's collection, use, and disclosure of personal data are beyond the framework's scope.

2. *Amend Laws That Create Inconsistent or Confusing Requirements*

Because existing Federal laws treat similar technologies within the communications sector differently,[49] the Administration supports simplifying and clarifying the legal landscape and making the FTC responsible for enforcing the Consumer Privacy Bill of Rights against communications providers.

F. Set a National Standard for Security Breach Notification

In the specific area of security breaches, the Administration supports creating a national standard under which companies must notify consumers of unauthorized disclosures of certain kinds of personal data. Security breach notification (SBN) laws effectively promote the protection of sensitive personal data. They require companies in certain situations to notify consumers whose personal data was exposed to unauthorized recipients. Notice helps consumers protect themselves against harms such as identity theft. It also provides companies with incentives to establish better data security in the first place. The SBN model is also gaining acceptance internationally as a performance-based requirement that effectively protects consumers.

Currently, 47 States, the District of Columbia, and several U.S. Territories, have SBN laws. Variations in States have allowed a sense of the most effective approaches to emerge, but the need for national uniformity is now evident. The patchwork of State laws creates significant burdens for companies without much countervailing benefit for consumers. As part of its comprehensive cybersecurity legislative package, the Administration recommended creating a national standard for notifying consumers in the event that there are unauthorized disclosures of certain types of personal data.[50] This national standard would replace the various State standards that exist today and preempt future State legislation in this area.

49. *See*, e.g., 47 U.S.C. §§ 222, 338 & 551 (requiring telecommunications carriers, satellite carriers, and cable services, respectively, to protect customers' personal information).

50. The White House, Data Breach Notification Legislative Language, May 2011, http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/data-breach-notification.pdf.

VII. Federal Government Leadership in Improving Individual Privacy Protections

In areas other than consumer data privacy, the Administration is continuing the Federal government's long history of championing data privacy protections in the public and private spheres. This history stems from the early days of computerized data processing. In 1973, the Department of Health, Education, and Welfare (HEW) Advisory Committee on Automated Personal Data Systems issued a report entitled Records, Computers, and the Rights of Citizens. This landmark report provided an early statement of the FIPPs that provide a foundation for the Administration's Consumer Privacy Bill of Rights.

Since then, the Federal government has led the way in demonstrating that protecting privacy is integral to conducting the Nation's business. No single event or policy need has spurred this activity. In some cases, Federal agencies consider privacy issues in response to specific Congressional mandates. In other cases, Federal agencies integrate privacy into innovative initiatives that advance their core missions. The activities of Federal agencies with duties that range across a broad array of economic sectors—including healthcare, financial services, and education—illustrate the Administration's commitment to promoting best practices, enabling new services, providing tools to address many different privacy issues, and enforcing individual privacy rights.

A. Enabling New Services

Like the private sector, Federal agencies must confront data privacy issues when delivering services to the public. A particularly challenging set of privacy issues arises in connection with delivering healthcare to the Nation's veterans. The Department of Veterans Affairs (VA) provides healthcare for 8.3 million enrolled veterans through more than 1,400 facilities distributed across the Nation. To help manage a healthcare operation of this scale and scope efficiently and cost-effectively, the VA is continuing to incorporate information technology into its healthcare delivery system. Protecting the privacy of veterans' health information is essential to the success of this endeavor.

VA recently launched an initiative that demonstrates how careful attention to privacy and security protections for personal health information can lead to significant advances in how healthcare is delivered. VA incorporated privacy and security protections into its "My HealtheVet Personal Health Record." This system is a gateway to information that helps veterans to enable their caregivers to deliver better care and provides other Internet-based tools that empower veterans to become active partners in their health care. The VA's Blue Button service allows veterans to download an electronic copy of their HealtheVet information in a secure manner.

How Administration Action Is Enabling Privacy in Other Areas

- **Integrating Privacy into Cybersecurity Initiatives.** Protecting privacy is a priority in the Administration's efforts to secure online environments for continuing increases in productivity, innovation, and support for new business ventures. Led by the National Institute of Standards and Technology (NIST), the *National Strategy for Trusted Identities in Cyberspace* calls for a partnership with the commercial sector to develop more standardized, secure, and privacy-enhancing ways to authenticate individuals online.
- **Enhancing Transparency in Credit Markets.** The Administration is ensuring that privacy protections keep pace with developments in uses of personal data in setting the terms of consumer credit. The Federal Reserve Board, together with the FTC, issued a rule that requires creditors to provide a consumer with notice when, based on the consumer's credit report, the creditor provides credit to the consumer on less favorable terms than it provides to other consumers. This rule also entitles consumers who are notified of such "risk-based pricing" to obtain a free credit report, so that they can check whether the information creditors use is accurate.

B. Protecting Privacy Through Effective Enforcement

The FTC has used its civil enforcement authority against those commercial enterprises that fail to follow Commission rules or act in an unfair or deceptive manner. Since 2009, the FTC has taken actions against companies that have failed to exercise reasonable care to secure sensitive personal and medical information, represented that they abide by the U.S.-EU or U.S.-Swiss Safe Harbor agreements when they do not or they have allowed these certifications to lapse, or that misrepresent the use of tracking software. The FTC also prosecuted actions involving deceptive practices by online seal providers, social media companies, and companies claiming to protect identities. In addition, the FTC prosecuted cases under the Telemarketing Sales Rule, the COPPA Rule, the Fair Credit Reporting Act, and the GLB Safeguards Rule.

The Administration also takes enforcing statutory privacy rights seriously. Federal agencies with law enforcement authority have taken action against those who violate privacy rights. For example, the Department of Justice (DOJ) aggressively prosecutes cases involving identity theft—the use of misappropriated personal data that can cause life-disrupting and economically devastating harm to its victims. In 2010 alone, DOJ's United States Attorneys' Offices prosecuted nearly 1300 cases involving identity theft, and U.S. Attorneys have brought nearly 700 identity theft cases in the current fiscal year. DOJ, assisted by investigators from the Federal Bureau of Investigation and Department of Homeland Security (DHS) components such as United States Secret Service and U.S. Immigration and Customs Enforcement, also vigorously prosecutes individuals who obtain personal data (and other information) by breaking into computers. Taken together, these efforts help protect the confidentiality of personal data and bring justice for victims of identity theft and other crimes that involve the misuse of personal data.

C. Guidance for Protecting Privacy

Federal agencies are also devoting resources to producing guidance on data privacy that has broad applicability in the private sector. The Department of Health and Human Services (HHS), for example, has issued guidance that analyzes some of the fundamental issues surrounding responses to security breaches that involve personally identifiable information. In 2009, the Department of Health and Human Services Office for Civil Rights (OCR) issued guidance on when health information is considered to be secure (and therefore exempt from breach notification requirements) by specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable. In 2010, OCR also issued guidance on conducting a risk analysis under the HIPAA Security Rule. OCR plans to issue additional guidance on the HIPAA Privacy Rule's "minimum necessary" standard and on de-identification of health information under the HIPAA Privacy Rule.

Federal agencies are also providing guidance on how to make more effective use of existing privacy-protecting measures. In 2009, eight Federal agencies released a model privacy notice form that financial institutions can opt to use for their privacy notices to consumers required by GLB. Use of the model form provides a legal safe harbor for compliance with the GLB Privacy Rule, though the model form is not required. The agencies conducted extensive consumer research and testing in developing the model form to ensure that consumers can easily understand what financial institutions do with their personal information and compare different institutions' information sharing practices.

Other Significant Administration Guidance on Privacy:

- **Raising Public Awareness of Privacy and Data Security.** DHS is leading a national public awareness effort called *Stop. Think. Connect.* to inform the American public of the need to strengthen cybersecurity and to provide practical tips to help Americans increase their safety and security online. In addition, the FTC has issued guides explaining measures that consumers and companies can take to protect children's privacy online, minimize the risk of medical identity theft, and prevent the loss of sensitive data through peer-to-peer file sharing applications.
- **Applying Privacy Principles to New Technologies.** The Administration is demonstrating that the same privacy principles that inform the general consumer data privacy framework developed here also apply to specific, emerging contexts. The "Smart Grid"—the incorporation of information technologies to make the electric grid more efficient, more accommodating of clean sources of energy, and a source of new jobs and innovation—provides an excellent example. Over the past two years, the Department of Energy and the National Institute of Standards and Technology engaged with stakeholders to understand privacy issues that could arise from this promising new technology. This work culminated in the Administration's *Policy Framework for The 21st Century Grid: Enabling Our Secure Energy Future*, which recommends that States make comprehensive FIPPs the starting point for protecting the detailed energy usage data that the Smart Grid will generate.

D. Integrating Privacy Into the Structure of Federal Agencies

Finally, Federal agencies are leading the way in incorporating privacy into their structure and operations and in developing accountable organizations. Some of these accountability-enhancing practices and tools have diffused to the private sector and across the globe. For example, the Internal Revenue Service and DHS pioneered the use of privacy impact assessments (PIAs), which provide for structured assessments of the potential privacy issues arising from new information systems and, under the E-Government Act of 2002, are now required of Federal agencies under some circumstances. Building on efforts of previous Administrations, this Administration has extended the use of PIAs to social media. Since their initial development within the Federal government, PIAs have become widely used in the private sector and within the European Union. Federal agencies also continue to make privacy professionals part of their senior leadership structures. Many Federal agencies have full-time, professional chief privacy officers, who engage on privacy issues within their agencies, in broader discussions within the Federal government, and with the general public.

VIII. Conclusion

The United States is committed to protecting privacy. It is an element of individual dignity and an aspect of participation in democratic society. To an increasing extent, privacy protections have become critical to the information-based economy. Stronger consumer data privacy protections will buttress the trust that is necessary to promote the full economic, social, and political uses of networked technologies. The increasing quantities of personal data that these technologies subject to collection, use, and disclosure have fueled innovation and significant social benefits. We can preserve these benefits while also ensuring that our consumer data privacy policy better reflects the value that Americans place on privacy and bolsters trust in the Internet and other networked technologies.

The framework set forth in the preceding pages provides a way to achieve these goals. The Consumer Privacy Bill of Rights should be the legal baseline that governs consumer data privacy in the United States. The Administration will work with Congress to bring this about, but it will also work with private-sector stakeholders to adopt the Consumer Privacy Bill of Rights in the absence of legislation. To encourage adoption, the Department of Commerce will convene multistakeholder processes to encourage the development of enforceable, context-specific codes of conduct. The United States Government will engage with our international partners to increase the interoperability of our respective consumer data privacy frameworks. Federal agencies will continue to develop innovative privacy-protecting programs and guidance as well as enforce the broad array of existing Federal laws that protect consumer privacy.

A cornerstone of this framework is its call for the ongoing participation of private-sector stakeholders. The views that companies, civil society, academics, and advocates provided to the Administration through written comments, public symposia, and informal discussions have been invaluable in shaping this framework. Implementing it, and making progress toward consumer data privacy protections that support a more trustworthy networked world, will require all of us to continue to work together.

Appendix A: The Consumer Privacy Bill of Rights

CONSUMER PRIVACY BILL OF RIGHTS

The Consumer Privacy Bill of Rights applies to *personal data*, which means any data, including aggregations of data, which is linkable to a specific individual. Personal data may include data that is linked to a specific computer or other device. The Administration supports Federal legislation that adopts the principles of the Consumer Privacy Bill of Rights. Even without legislation, the Administration will convene multistakeholder processes that use these rights as a template for codes of conduct that are enforceable by the Federal Trade Commission. These elements—the Consumer Privacy Bill of Rights, codes of conduct, and strong enforcement—will increase interoperability between the U.S. consumer data privacy framework and those of our international partners.

1. **INDIVIDUAL CONTROL: Consumers have a right to exercise control over what personal data companies collect from them and how they use it.** Companies should provide consumers appropriate control over the personal data that consumers share with others and over how companies collect, use, or disclose personal data. Companies should enable these choices by providing consumers with easily used and accessible mechanisms that reflect the scale, scope, and sensitivity of the personal data that they collect, use, or disclose, as well as the sensitivity of the uses they make of personal data. Companies should offer consumers clear and simple choices, presented at times and in ways that enable consumers to make meaningful decisions about personal data collection, use, and disclosure. Companies should offer consumers means to withdraw or limit consent that are as accessible and easily used as the methods for granting consent in the first place.

2. **TRANSPARENCY: Consumers have a right to easily understandable and accessible information about privacy and security practices.** At times and in places that are most useful to enabling consumers to gain a meaningful understanding of privacy risks and the ability to exercise Individual Control, companies should provide clear descriptions of what personal data they collect, why they need the data, how they will use it, when they will delete the data or de-identify it from consumers, and whether and for what purposes they may share personal data with third parties.

3. **RESPECT FOR CONTEXT: Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.** Companies should limit their use and disclosure of personal data to those purposes that are consistent with both the relationship that they have with consumers and the context in which consumers originally disclosed the data, unless required by law to do otherwise. If companies will use or disclose personal data for other purposes, they should provide heightened Transparency and Individual Control by disclosing these other purposes in a manner that is prominent and easily actionable by consumers at the time of data collection. If,

subsequent to collection, companies decide to use or disclose personal data for purposes that are inconsistent with the context in which the data was disclosed, they must provide heightened measures of Transparency and Individual Choice. Finally, the age and familiarity with technology of consumers who engage with a company are important elements of context. Companies should fulfill the obligations under this principle in ways that are appropriate for the age and sophistication of consumers. In particular, the principles in the Consumer Privacy Bill of Rights may require greater protections for personal data obtained from children and teenagers than for adults.

4. **SECURITY: Consumers have a right to secure and responsible handling of personal data.** Companies should assess the privacy and security risks associated with their personal data practices and maintain reasonable safeguards to control risks such as loss; unauthorized access, use, destruction, or modification; and improper disclosure.

5. **ACCESS AND ACCURACY: Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.** Companies should use reasonable measures to ensure they maintain accurate personal data. Companies also should provide consumers with reasonable access to personal data that they collect or maintain about them, as well as the appropriate means and opportunity to correct inaccurate data or request its deletion or use limitation. Companies that handle personal data should construe this principle in a manner consistent with freedom of expression and freedom of the press. In determining what measures they may use to maintain accuracy and to provide access, correction, deletion, or suppression capabilities to consumers, companies may also consider the scale, scope, and sensitivity of the personal data that they collect or maintain and the likelihood that its use may expose consumers to financial, physical, or other material harm.

6. **FOCUSED COLLECTION: Consumers have a right to reasonable limits on the personal data that companies collect and retain.** Companies should collect only as much personal data as they need to accomplish purposes specified under the Respect for Context principle. Companies should securely dispose of or de-identify personal data once they no longer need it, unless they are under a legal obligation to do otherwise.

7. **ACCOUNTABILITY: Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.** Companies should be accountable to enforcement authorities and consumers for adhering to these principles. Companies also should hold employees responsible for adhering to these principles. To achieve this end, companies should train their employees as appropriate to handle personal data consistently with these principles and regularly evaluate their performance in this regard. Where appropriate, companies should conduct full audits. Companies that disclose personal data to third parties should at a minimum ensure that the recipients are under enforceable contractual obligations to adhere to these principles, unless they are required by law to do otherwise.

Appendix B: Comparison of the Consumer Privacy Bill of Rights to Other Statements of the Fair Information Practice Principles (FIPPs)

Consumer Privacy Bill of Rights	OECD Privacy Guidelines (excerpts)	DHS Privacy Policy (generalized)	APEC Principles (excerpts)
Individual Control. Consumers have a right to exercise control over what personal data that companies collect from them and how they use it.	**Use Limitation Principle.** Personal data should not be disclosed . . . except "with the consent of the data subject or by the authority of law."	**Individual Participation.** Organizations should involve the individual in the process of using PII [personally identifiable information] and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII.	**Choice.** Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information.
Transparency. Consumers have a right to easily understandable information about privacy and security practices.	**Openness Principle.** There should be a general policy of openness about developments, practices and policies with respect to personal data.	**Transparency.** Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of PII.	**Notice.** Personal information controllers should provide clear and easily accessible statements about their practices and policies . . . .

Consumer Privacy Bill of Rights	OECD Privacy Guidelines (excerpts)	DHS Privacy Policy (generalized)	APEC Principles (excerpts)
Respect for Context. Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.	**Purpose Specification Principle.** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.	**Purpose Specification.** Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.	**Notice.** All reasonably practicable steps shall be taken to ensure that such notice is provided either before or at the time of collection of personal information. Otherwise, such notice should be provided as soon after as is practicable.
	Use Limitation Principle. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 [purpose specification] except . . . (a) with the consent of the data subject; or (b) by the authority of law.	**Use Limitation.** Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.	**Uses of Personal Information.** Personal information collected should be used only to fulfill the purposes of collection and other compatible or related purposes except: a) with the consent of the individual whose personal information is collected; b) when necessary to provide a service or product requested by the individual; or, c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect.
Security. Consumers have a right to secure and responsible handling of personal data.	**Security Safeguards Principle.** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.	**Security.** Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.	**Security Safeguards.** Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses.

APPENDIX B: COMPARISON OF THE CONSUMER PRIVACY BILL OF RIGHTS TO OTHER STATEMENTS OF THE FAIR INFORMATION PRACTICE PRINCIPLES (FIPPS)

Consumer Privacy Bill of Rights	OECD Privacy Guidelines (excerpts)	DHS Privacy Policy (generalized)	APEC Principles (excerpts)
Access and Accuracy. Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.	**Individual Participation Principle.** An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.	**Data Quality and Integrity.** Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.	**Access and Correction.** Individuals should be able to: a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them; b) have communicated to them, after having provided sufficient proof of their identity, personal information about them; i. within a reasonable time ii. at a charge, if any, that is not excessive; iii. in a reasonable manner; iv. in a form that is generally understandable; and, c) challenge the accuracy of information relating to them and, if possible and as appropriate, have the information rectified, completed, amended or deleted.
	Data Quality Principle. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.		**Integrity of Personal Information.** Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.
			Preventing Harm. Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information.

Consumer Privacy Bill of Rights	OECD Privacy Guidelines (excerpts)	DHS Privacy Policy (generalized)	APEC Principles (excerpts)
Focused Collection: Consumers have a right to reasonable limits on the personal data that companies collect and retain.	**Collection Limitation Principle.** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.	**Data Minimization:** Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).	**Collection Limitation.** The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.
Accountability. Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.	**Accountability Principle.** A data controller should be accountable for complying with measures which give effect to the principles stated above.	**Accountability and Auditing:** Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.	**Accountability.** A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.

Read 11/16 Plore

Protecting Consumer Privacy in an Era of Rapid Change

RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS

FTC REPORT

FEDERAL TRADE COMMISSION | MARCH 2012

Protecting Consumer Privacy in an Era of Rapid Change

RECOMMENDATIONS FOR
BUSINESSES AND POLICYMAKERS

FTC REPORT
MARCH 2012

CONTENTS

EXECUTIVE SUMMARY

In today's world of smart phones, smart grids, and smart cars, companies are collecting, storing, and sharing more information about consumers than ever before. Although companies use this information to innovate and deliver better products and services to consumers, they should not do so at the expense of consumer privacy.

With this Report, the Commission calls on companies to act now to implement best practices to protect consumers' private information. These best practices include making privacy the "default setting" for commercial data practices and giving consumers greater control over the collection and use of their personal data through simplified choices and increased transparency. Implementing these best practices will enhance trust and stimulate commerce.

This Report follows a preliminary staff report that the Federal Trade Commission ("FTC" or "Commission") issued in December 2010. The preliminary report proposed a framework for protecting consumer privacy in the 21st Century. Like this Report, the framework urged companies to adopt the following practices, consistent with the Fair Information Practice Principles first articulated almost 40 years ago:

- **Privacy by Design:** Build in privacy at every stage of product development;
- **Simplified Choice for Businesses and Consumers:** Give consumers the ability to make decisions about their data at a relevant time and context, including through a Do Not Track mechanism, while reducing the burden on businesses of providing unnecessary choices; and
- **Greater Transparency:** Make information collection and use practices transparent.

The Commission received more than 450 public comments in response to the preliminary report from various stakeholders, including businesses, privacy advocates, technologists and individual consumers. A wide range of stakeholders, including industry, supported the principles underlying the framework, and many companies said they were already following them. At the same time, many commenters criticized the slow pace of self-regulation, and argued that it is time for Congress to enact baseline privacy legislation. In this Report, the Commission addresses the comments and sets forth a revised, final privacy framework that adheres to, but also clarifies and fine-tunes, the basic principles laid out in the preliminary report.

Since the Commission issued the preliminary staff report, Congress has introduced both general privacy bills and more focused bills, including ones addressing Do Not Track and the privacy of teens. Industry has made some progress in certain areas, most notably, in responding to the preliminary report's call for Do Not Track. In other areas, however, industry progress has been far slower. Thus, overall, consumers do not yet enjoy the privacy protections proposed in the preliminary staff report.

The Administration and certain Members of Congress have called for enactment of baseline privacy legislation. The Commission now also calls on Congress to consider enacting baseline privacy legislation and reiterates its call for data security legislation. The Commission is prepared to work with Congress and other stakeholders to craft such legislation. At the same time, the Commission urges industry to accelerate the pace of self-regulation.

The remainder of this Executive Summary describes key developments since the issuance of the preliminary report, discusses the most significant revisions to the proposed framework, and lays out several next steps.

DEVELOPMENTS SINCE ISSUANCE OF THE PRELIMINARY REPORT

In the last 40 years, the Commission has taken numerous actions to shape the consumer privacy landscape. For example, the Commission has sued dozens of companies that broke their privacy and security promises, scores of telemarketers that called consumers on the Do Not Call registry, and more than a hundred scammers peddling unwanted spam and spyware. Since it issued the initial staff report, the Commission has redoubled its efforts to protect consumer privacy, including through law enforcement, policy advocacy, and consumer and business education. It has also vigorously promoted self-regulatory efforts.

On the law enforcement front, since December 2010, the Commission:

- Brought enforcement actions against Google and Facebook. The orders obtained in these cases require the companies to obtain consumers' affirmative express consent before materially changing certain of their data practices and to adopt strong, company-wide privacy programs that outside auditors will assess for 20 years. These orders will protect the more than one billion Google and Facebook users worldwide.
- Brought enforcement actions against online advertising networks that failed to honor opt outs. The orders in these cases are designed to ensure that when consumers choose to opt out of tracking by advertisers, their choice is effective.
- Brought enforcement actions against mobile applications that violated the Children's Online Privacy Protection Act as well as applications that set default privacy settings in a way that caused consumers to unwittingly share their personal data.
- Brought enforcement actions against entities that sold consumer lists to marketers in violation of the Fair Credit Reporting Act.
- Brought actions against companies for failure to maintain reasonable data security.

On the policy front, since December 2010, the FTC and staff:

- Hosted two privacy-related workshops, one on child identity theft and one on the privacy implications of facial recognition technology.
- Testified before Congress ~~ten times~~ on privacy and data security issues.
- Consulted with other federal agencies, including the Federal Communications Commission, the Department of Health and Human Services, and the Department of Commerce, on their privacy initiatives. The Commission has supported the Department of Commerce's initiative to convene stakeholders to develop privacy-related codes of conduct for different industry sectors.
- Released a survey of data collection disclosures by mobile applications directed to children.
- Proposed amendments to the Children's Online Privacy Protection Act Rule.

Oh cool

Can agencies propose law like changes

On the education front, since December 2010, the Commission:

- Continued outreach efforts through the FTC's consumer online safety portal, OnGuardOnline.gov, which provides information in a variety of formats – articles, games, quizzes, and videos – to help consumers secure their computers and protect their personal information. It attracts approximately 100,000 unique visitors per month.
- Published new consumer education materials on identity theft, Wi-Fi hot spots, cookies, and mobile devices.
- Sent warning letters to marketers of mobile apps that do background checks on individuals, educating them about the requirements of the Fair Credit Reporting Act.

To promote self-regulation, since December 2010, the Commission:

- Continued its call for improved privacy disclosures and choices, particularly in the area of online behavioral tracking. In response to this call, as well as to Congressional interest:
  - A number of Internet browser vendors developed browser-based tools for consumers to request that websites not track their online activities.
  - The World Wide Web Consortium, an Internet standard setting organization, is developing a universal web protocol for Do Not Track.
  - The Digital Advertising Alliance ("DAA"), a coalition of media and marketing organizations, has developed a mechanism, accessed through an icon that consumers can click, to obtain information about and opt out of online behavioral advertising. Additionally, the DAA has committed to preventing the use of consumers' data for secondary purposes like credit and employment and honoring the choices about tracking that consumers make through the settings on their browsers.
- Participated in the development of enforceable cross-border privacy rules for businesses to harmonize and enhance privacy protection of consumer data that moves between member countries of the forum on Asia Pacific Economic Cooperation.

THE FINAL REPORT

Based upon its analysis of the comments filed on the proposed privacy framework, as well as commercial and technological developments, the Commission is issuing this final Report. The final framework is intended to articulate best practices for companies that collect and use consumer data. These best practices can be useful to companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses. The final privacy framework contained in this Report is also intended to assist Congress as it considers privacy legislation. To the extent the framework goes beyond existing legal requirements, the framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC. While retaining the proposed framework's fundamental best practices of privacy by design, simplified choice, and greater transparency, the Commission makes revised recommendations in three key areas in response to the comments.

First, the Commission makes changes to the framework's scope. The preliminary report proposed that the privacy framework apply to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device. To address concerns about undue burdens on small businesses, the final framework does not apply to companies that collect only non-sensitive data from fewer than 5,000 consumers a year, provided they do not share the data with third parties. Commenters also expressed concern that, with improvements in technology and the ubiquity of public information, more and more data could be "reasonably linked" to a consumer, computer or device, and that the proposed framework provided less incentive for a business to try to de-identify the data it maintains. To address this issue, the Report clarifies that data is not "reasonably linkable" to the extent that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data.

Second, the Commission revises its approach to how companies should provide consumers with privacy choices. To simplify choice for both consumers and businesses, the proposed framework set forth a list of five categories of "commonly accepted" information collection and use practices for which companies need not provide consumers with choice (product fulfillment, internal operations, fraud prevention, legal compliance and public purpose, and first-party marketing). Several business commenters expressed concern that setting these "commonly accepted practices" in stone would stifle innovation. Other commenters expressed the concern that the "commonly accepted practices" delineated in the proposed framework were too broad and would allow a variety of practices to take place without consumer consent.

In response to these concerns, the Commission sets forth a modified approach that focuses on the context of the consumer's interaction with the business. Under this approach, companies do not need to provide choice before collecting and using consumers' data for practices that are consistent with the context of the transaction, consistent with the company's relationship with the consumer, or as required or specifically authorized by law. Although many of the five "commonly accepted practices" identified in the preliminary report would generally meet this standard, there may be exceptions. The Report provides examples of how this new "context of the interaction" standard would apply in various circumstances.

Third, the Commission recommends that Congress consider enacting targeted legislation to provide greater transparency for, and control over, the practices of information brokers. The proposed framework recommended that companies provide consumers with reasonable access to the data the companies maintain about them, proportionate to the sensitivity of the data and the nature of its use. Several commenters discussed in particular the importance of consumers' ability to access information that information brokers have about them. These commenters noted the lack of transparency about the practices of information brokers, who often buy, compile, and sell a wealth of highly personal information about consumers but never interact directly with them. Consumers are often unaware of the existence of these entities, as well as the purposes for which they collect and use data.

The Commission agrees that consumers should have more control over the practices of information brokers and believes that appropriate legislation could help address this goal. Any such legislation could be

modeled on a bill that the House passed on a bipartisan basis during the 111th Congress, which included a procedure for consumers to access and dispute personal data held by information brokers.

IMPLEMENTATION OF THE PRIVACY FRAMEWORK

While Congress considers privacy legislation, the Commission urges industry to accelerate the pace of its self-regulatory measures to implement the Commission's final privacy framework. Although some companies have excellent privacy and data security practices, industry as a whole must do better. Over the course of the next year, Commission staff will promote the framework's implementation by focusing its policymaking efforts on five main action items, which are highlighted here and discussed further throughout the report.

- **Do Not Track:** As discussed above, industry has made significant progress in implementing Do Not Track. The browser vendors have developed tools that consumers can use to signal that they do not want to be tracked; the Digital Advertising Alliance ("DAA") has developed its own icon-based tool and has committed to honor the browser tools; and the World Wide Web Consortium ("W3C") has made substantial progress in creating an international standard for Do Not Track. However, the work is not done. The Commission will work with these groups to complete implementation of an easy-to use, persistent, and effective Do Not Track system.
- **Mobile:** The Commission calls on companies providing mobile services to work toward improved privacy protections, including the development of short, meaningful disclosures. To this end, FTC staff has initiated a project to update its business guidance about online advertising disclosures. As part of this project, staff will host a workshop on May 30, 2012 and will address, among other issues, mobile privacy disclosures and how these disclosures can be short, effective, and accessible to consumers on small screens. The Commission hopes that the workshop will spur further industry self-regulation in this area.
- **Data Brokers:** To address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information, the Commission supports targeted legislation – similar to that contained in several of the data security bills introduced in the 112th Congress – that would provide consumers with access to information about them held by a data broker. To further increase transparency, the Commission calls on data brokers that compile data for marketing purposes to explore creating a centralized website where data brokers could (1) identify themselves to consumers and describe how they collect and use consumer data and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain.
- **Large Platform Providers:** To the extent that large platforms, such as Internet Service Providers, operating systems, browsers, and social media seek, to comprehensively track consumers' online activities, it raises heightened privacy concerns. To further explore privacy and other issues related to this type of comprehensive tracking, FTC staff intends to host a public workshop in the second half of 2012.

- **Promoting Enforceable Self-Regulatory Codes:** The Department of Commerce, with the support of key industry stakeholders, is undertaking a project to facilitate the development of sector-specific codes of conduct. FTC staff will participate in that project. To the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work. The Commission will also continue to enforce the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join.

FINAL FTC PRIVACY FRAMEWORK AND IMPLEMENTATION RECOMMENDATIONS

The final privacy framework is intended to articulate best practices for companies that collect and use consumer data. These best practices can be useful to companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses. The final privacy framework contained in this report is also intended to assist Congress as it considers privacy legislation. To the extent the framework goes beyond existing legal requirements, the framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC.

SCOPE

Final Scope: The framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device, unless the entity collects only non-sensitive data from fewer than 5,000 consumers per year and does not share the data with third parties.

PRIVACY BY DESIGN

Baseline Principle: Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services.

A. The Substantive Principles

what does this mean?

Final Principle: Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy.

B. Procedural Protections to Implement the Substantive Principles

Final Principle: Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.

SIMPLIFIED CONSUMER CHOICE

Baseline Principle: Companies should simplify consumer choice.

A. Practices That Do Not Require Choice

Final Principle: Companies do not need to provide choice before collecting and using consumer data for practices that are consistent with the context of the transaction or the company's relationship with the consumer, or are required or specifically authorized by law.

To balance the desire for flexibility with the need to limit the types of practices for which choice is not required, the Commission has refined the final framework so that companies engaged in practices consistent with the context of their interaction with consumers need not provide choices for those practices.

I liked the WH one better...

B. Companies Should Provide Consumer Choice for Other Practices

Final Principle: For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data. Companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes.

The Commission commends industry's efforts to improve consumer control over online behavioral tracking by developing a Do Not Track mechanism, and encourages continued improvements and full implementation of those mechanisms.

TRANSPARENCY

Baseline Principle: Companies should increase the transparency of their data practices.

A. Privacy notices

Final Principle: Privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices.

B. Access

Final Principle: Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use.

The Commission has amplified its support for this principle by including specific recommendations governing the practices of information brokers.

C. Consumer Education

Final Principle: All stakeholders should expand their efforts to educate consumers about commercial data privacy practices.

LEGISLATIVE RECOMMENDATIONS

The Commission now also calls on Congress to consider enacting baseline privacy legislation and reiterates its call for data security and data broker legislation. The Commission is prepared to work with Congress and other stakeholders to craft such legislation. At the same time, the Commission urges industry to accelerate the pace of self-regulation.

FTC WILL ASSIST WITH IMPLEMENTATION IN FIVE KEY AREAS

As discussed throughout the Commission's final Report, there are a number of specific areas where policy makers have a role in assisting with the implementation of the self-regulatory principles that make up the final privacy framework. Areas where the FTC will be active over the course of the next year include the following:

1. Do Not Track

Industry has made significant progress in implementing Do Not Track. The browser vendors have developed tools that consumers can use to signal that they do not want to be tracked; the DAA has developed its own icon-based tool and has committed to honor the browser tools; and the W3C has made substantial progress in creating an international standard for Do Not Track. However, the work is not done. The Commission will work with these groups to complete implementation of an easy-to use, persistent, and effective Do Not Track system.

2. Mobile

The Commission calls on companies providing mobile services to work toward improved privacy protections, including the development of short, meaningful disclosures. To this end, FTC staff has initiated a project to update its business guidance about online advertising disclosures. As part of this project, staff will host a workshop on May 30, 2012 and will address, among other issues, mobile privacy disclosures and how these disclosures can be short, effective, and accessible to consumers on small screens. The Commission hopes that the workshop will spur further industry self-regulation in this area.

3. Data Brokers

To address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information, the Commission supports targeted legislation – similar to that contained in several of the data security bills introduced in the 112th Congress – that would provide consumers with access to information about them held by a data broker. To further increase transparency, the Commission calls on data brokers that compile data for marketing purposes to explore creating a centralized website where data brokers could (1) identify themselves to consumers and describe how they collect and use consumer data and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain.

also inaccuracying wrong

4. Large Platform Providers

To the extent that large platforms, such as Internet Service Providers, operating systems, browsers, and social media, seek to comprehensively track consumers' online activities, it raises heightened privacy concerns. To further explore privacy and other issues related to this type of comprehensive tracking, FTC staff intends to host a public workshop in the second half of 2012.

ad cos?

interesting term—

5. Promoting Enforceable Self-Regulatory Codes

The Department of Commerce, with the support of key industry stakeholders, is undertaking a project to facilitate the development of sector-specific codes of conduct. FTC staff will participate in that project. To the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work. The Commission will also continue to enforce the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join.

What about spammy cos that don't do this

In all other areas, the Commission calls on individual companies, trade associations, and self-regulatory bodies to adopt the principles contained in the final privacy framework, to the extent they have not already done so. For its part, the FTC will focus its policy efforts on the five areas identified above, vigorously enforce existing laws, work with industry on self-regulation, and continue to target its education efforts on building awareness of existing data collection and use practices and the tools to control them.

I. INTRODUCTION

In December 2010, the Federal Trade Commission ("FTC" or "Commission") issued a preliminary staff report to address the privacy issues associated with new technologies and business models.[1] The report outlined the FTC's 40-year history of promoting consumer privacy through policy and enforcement work, discussed the themes and areas of consensus that emerged from the Commission's "Exploring Privacy" roundtables, and set forth a proposed framework to guide policymakers and other stakeholders regarding best practices for consumer privacy. The proposed framework called on companies to build privacy protections into their business operations (*i.e.*, adopt "privacy by design"[2]), offer simplified choice mechanisms that give consumers more meaningful control, and increase the transparency of their data practices.

The preliminary report included a number of questions for public comment to assist and guide the Commission in developing a final privacy framework. The Commission received more than 450 comments from a wide variety of interested parties, including consumer and privacy advocates, individual companies and trade associations, academics, technologists, and domestic and foreign government agencies. Significantly, more than half of the comments came from individual consumers. The comments have helped the Commission refine the framework to better protect consumer privacy in today's dynamic and rapidly changing marketplace.

In this Final Report, the Commission adopts staff's preliminary framework with certain clarifications and revisions. The final privacy framework is intended to articulate best practices for companies that collect and use consumer data. These best practices can be useful to companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses. The final privacy framework contained in this Report is also intended to assist Congress as it considers privacy legislation. To the extent the framework goes beyond existing legal requirements, the framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC.

The Report highlights the developments since the FTC issued staff's preliminary report, including the Department of Commerce's parallel privacy initiative, proposed legislation, and actions by industry and other stakeholders. Next, it analyzes and responds to the main issues raised by the public comments. Based on those comments, as well as marketplace developments, the Report sets forth a revised privacy framework and legislative recommendations. Finally, the Report outlines a series of policy initiatives that FTC staff will undertake in the next year to assist industry with implementing the final framework as best practices.

---

1 FTC, *Protecting Consumer Privacy in an Era of Rapid Change, A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report* (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

2 Privacy by Design is an approach that Ann Cavoukian, Ph.D., Information and Privacy Commissioner, Ontario, Canada, has advocated. *See* Information and Privacy Commissioner, Ontario, Canada, Privacy by Design, http://privacybydesign.ca/.

II. BACKGROUND

A. FTC ROUNDTABLES AND PRELIMINARY STAFF REPORT

Between December 2009 and March 2010, the FTC convened its "Exploring Privacy" roundtables.[3] The roundtables brought together stakeholders representing diverse interests to evaluate whether the FTC's existing approach to protecting consumer privacy was adequate in light of 21st Century technologies and business models. From these discussions, as well as submitted materials, a number of themes emerged. First, the collection and commercial use of consumer data in today's society is ubiquitous and often invisible to consumers. Second, consumers generally lack full understanding of the nature and extent of this data collection and use and, therefore, are unable to make informed choices about it. Third, despite this lack of understanding, many consumers are concerned about the privacy of their personal information. Fourth, the collection and use of consumer data has led to significant benefits in the form of new products and services. Finally, the traditional distinction between personally identifiable information and "anonymous" data has blurred.

Participants also pointed to shortcomings in existing frameworks that have attempted to address privacy concerns. The "notice-and-choice model," which encouraged companies to develop privacy policies describing their information collection and use practices, led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand.[4] The "harm-based model," which focused on protecting consumers from specific harms – physical security, economic injury, and unwarranted intrusions into their daily lives – had been criticized for failing to recognize a wider range of privacy-related concerns, including reputational harm or the fear of being monitored.[5] Participants noted that both of these privacy frameworks have struggled to keep pace with the rapid growth of technologies and business models that enable companies to collect and use consumers' information in ways that often are invisible to consumers.[6]

Building on the record developed at the roundtables and on its own enforcement and policymaking expertise, FTC staff proposed for public comment a framework for approaching privacy. The proposed framework included three major components. It called on companies to treat privacy as their "default setting" by implementing "privacy by design" throughout their regular business operations. The concept of privacy by design includes limitations on data collection and retention, as well as reasonable security and data accuracy. By considering and addressing privacy at every stage of product and service development,

What is it really?

3 The first roundtable took place on December 7, 2009, the second roundtable on January 28, 2010, and the third roundtable on March 17, 2010. *See* FTC, *Exploring Privacy – A Roundtable Series*, http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml.

4 *See, e.g., 1st Roundtable, Remarks of Fred Cate, Indiana University Maurer School of Law*, at 280-81; *1st Roundtable, Remarks of Lorrie Cranor, Carnegie Mellon University*, at 129; *see also Written Comment of Fred Cate, 2nd Roundtable, Consumer Protection in the Age of the 'Information Economy,'* cmt. #544506-00057, at 343-79.

5 *See, e.g., 1st Roundtable, Remarks of Marc Rotenberg, Electronic Privacy Information Center*, at 301; *1st Roundtable, Remarks of Leslie Harris, Center for Democracy & Technology*, at 36-38; *1st Roundtable, Remarks of Susan Grant, Consumer Federation of America*, at 38-39.

6 *See, e.g., 3rd Roundtable, Remarks of Kathryn Montgomery, American University School of Communication*, at 200-01; *2nd Roundtable, Remarks of Kevin Bankston, Electronic Frontier Foundation*, at 277.

companies can shift the burden away from consumers who would otherwise have to seek out privacy-protective practices and technologies. The proposed framework also called on companies to simplify consumer choice by presenting important choices – in a streamlined way – to consumers at the time they are making decisions about their data. As part of the call for simplified choice, staff asked industry to develop a mechanism that would allow consumers to more easily control the tracking of their online activities, often referred to as "Do Not Track." Finally, the framework focused on improving consumer understanding of commercial data practices ("transparency") and called on companies – both those that interact directly with consumers and those that lack a consumer interface – to improve the transparency of their practices. As discussed below, the Commission received a large number of thoughtful and informative comments regarding each of the framework's elements. These comments have allowed the Commission to refine the framework and to provide further guidance regarding its implementation.

B. DEPARTMENT OF COMMERCE PRIVACY INITIATIVES

In a related effort to examine privacy, in May 2010, the Department of Commerce ("DOC" or "Commerce") convened a public workshop to discuss how to balance innovation, commerce, and consumer privacy in the online context.[7] Based on the input received from the workshop, as well as related research, on December 16, 2010, the DOC published for comment a strategy paper outlining privacy recommendations and proposed initiatives.[8] Following the public comment period, on February 23, 2012, the Administration issued its final "White Paper" on consumer privacy. The White Paper recommends that Congress enact legislation to implement a Consumer Privacy Bill of Rights based on the Fair Information Practice Principles ("FIPPs").[9] In addition, the White Paper calls for a multistakeholder process to determine how to apply the Consumer Privacy Bill of Rights in different business contexts. Commerce issued a Notice of Inquiry on March 5, 2012, asking for public input on both the process for convening stakeholders on this project, as well as the proposed subject areas to be discussed.[10]

Staff from the FTC and Commerce worked closely to ensure that the agencies' privacy initiatives are complementary. Personnel from each agency actively participated in both the DOC and FTC initiatives, and have also communicated regularly on how best to develop a meaningful, effective, and consistent approach to privacy protection. Going forward, the agencies will continue to work collaboratively to guide implementation of these complementary privacy initiatives.

---

7 *See* Press Release, Department of Commerce, Commerce Secretary Gary Locke Discusses Privacy and Innovation with Leading Internet Stakeholders (May 7, 2010), *available at* http://www.commerce.gov/news/press-releases/2010/05/07/commerce-secretary-gary-locke-discusses-privacy-and-innovation-leadin.

8 *See* Department of Commerce Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (Dec. 16, 2010), *available at* http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf.

9 White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. The FIPPs as articulated in the Administration paper are: Transparency, Individual Control, Respect for Context, Security, Access, Accuracy, Focused Collection, and Accountability.

10 *See* National Telecommunications and Information Administration, Request for Public Comment, Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct, 77 Fed. Reg. 13098 (Mar. 5, 2012).

C. LEGISLATIVE PROPOSALS AND EFFORTS BY STAKEHOLDERS

Since Commission staff released its preliminary report in December 2010, there have been a number of significant legislative proposals, as well as steps by industry and other stakeholders, to promote consumer privacy.

1. DO NOT TRACK

The preliminary staff report called on industry to create and implement a mechanism to allow consumers to control the collection and use of their online browsing data, often referred to as "Do Not Track." Bills introduced in the House and the Senate specifically address the creation of Do Not Track mechanisms, and, if enacted, would mandate that the Commission promulgate regulations to establish standards for a Do Not Track regime.[11]

In addition to the legislative proposals calling for the creation of Do Not Track, staff's preliminary report recommendation triggered significant progress by various industry sectors to develop tools to allow consumers to control online tracking. A number of browser vendors – including Mozilla, Microsoft, and Apple – announced that the latest versions of their browsers permit consumers to instruct websites not to track their activities across websites.[12] Mozilla has also introduced a mobile browser for Android devices that enables Do Not Track.[13] The online advertising industry has also established an important program. The Digital Advertising Alliance ("DAA"), an industry coalition of media and marketing associations, has developed an initiative that includes an icon embedded in behaviorally targeted online ads.[14] When consumers click on the icon, they can see information about how the ad was targeted and delivered to them and they are given the opportunity to opt out of such targeted advertising. The program's recent growth and implementation has been significant. In addition, the DAA has committed to preventing the use of consumers' data for secondary purposes like credit and employment decisions. The DAA has also agreed to honor the choices about tracking that consumers make through settings on their web browsers. This will provide consumers two ways to opt out: through the DAA's icon in advertisements or through their browser settings. These steps demonstrate the online advertising industry's support for privacy and consumer choice.

---

11 *See* Do-Not-Track Online Act of 2011, S. 913, 112th Congress (2011); Do Not Track Me Online Act, H.R. 654, 112th Congress (2011).

12 *See* Press Release, Microsoft, Providing Windows Customers with More Choice and Control of Their Privacy Online with Internet Explorer 9 (Dec. 7, 2010), *available at* http://www.microsoft.com/presspass/features/2010/dec10/12-07ie9privacyqa.mspx; *Mozilla Firefox 4 Beta, Now Including "Do Not Track" Capabilities*, MOZILLA BLOG (Feb. 8, 2011), http://blog.mozilla.com/blog/2011/02/08/mozilla-firefox-4-beta-now-including-do-not-track-capabilities/; Nick Wingfield, *Apple Adds Do-Not-Track Tool to New Browser*, WALL ST. J., Apr. 13, 2011, *available at* http://online.wsj.com/article/SB10001424052748703551304576261272308358858.html. Google recently announced that it will also offer this capability in the next version of its browser. Gregg Kaizer, *FAQ: What Google's Do Not Track Move Means*, COMPUTERWORLD (Feb. 24, 2012), *available at* http://www.computerworld.com/s/article/9224583/FAQ_What_Google_s_Do_Not_Track_move_means.

13 *See* Mozilla, Do Not Track FAQs, http://dnt.mozilla.org.

14 *See* Press Release, Interactive Advertising Bureau, Major Marketing/Media Trade Groups Launch Program to Give Consumers Enhanced Control Over Collection and Use of Web Viewing Data for Online Behavioral Advertising (Oct. 4, 2010), *available at* http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-100410.

Finally, the World Wide Web Consortium ("W3C")[15] convened a working group to create a universal standard for Do Not Track. The working group includes DAA member companies, other U.S. and international companies, industry groups, and consumer groups. The W3C group has made substantial progress toward a standard that is workable in the desktop and mobile settings, and has published two working drafts of its standard documents. The group's goal is to complete a consensus standard in the coming months.

2. OTHER PRIVACY INITIATIVES

Beyond the Do Not Track developments, broader initiatives to improve consumer privacy are underway in Congress, Federal agencies, and the private sector. For example, Congress is considering several general privacy bills that would establish a regulatory framework for protecting consumer privacy by improving transparency about the commercial uses of personal information and providing consumers with choice about such use.[16] The bills would also provide the Commission rulemaking authority concerning, among other things, notice, consent, and the transfer of information to third parties.

In the House of Representatives, Members have introduced bipartisan legislation to amend the Children's Online Privacy Protection Act[17] ("COPPA") and establish other protections for children and teens.[18] The bill would prohibit the collection and use of minors' information for targeted marketing and would require websites to permit the deletion of publicly available information of minors. Members of Congress also introduced a number of other bills addressing data security and data breach notification in 2011.[19]

---

15 The W3C is an international standard-setting body that works "to lead the World Wide Web to its full potential by developing protocols and guidelines that ensure the long-term growth of the Web." *See* W3C Mission, http://www.w3.org/Consortium/mission.html.

16 *See* Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Congress (2011); Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act, H.R. 611, 112th Congress (2011); Consumer Privacy Protection Act of 2011, H.R. 1528, 112th Congress (2011).

17 Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506.

18 *See* Do Not Track Kids Act of 2011, H.R. 1895, 112th Congress (2011). In September 2011, the Commission issued a Notice of Proposed Rulemaking, proposing changes to the COPPA Rule to address changes in technology. *See FTC Children's Online Privacy Protection Rule*, 76 Fed. Reg. 59804 (proposed Sep. 27, 2011), *available at* http://www.ftc.gov/os/2011/09/110915coppa.pdf.

19 *See* Personal Data Privacy and Security Act of 2011, S. 1151, 112th Congress (2011); Data Security and Breach Notification Act of 2011, S. 1207, 112th Congress (2011); Data Breach Notification Act of 2011, S.1408, 112th Congress (2011); Data Security Act of 2011, S.1434, 112th Congress (2011); Personal Data Protection and Breach Accountability Act of 2011, S. 1535, 112th Congress (2011); Data Accountability and Trust Act, H.R. 1707, 112th Congress (2011); Data Accountability and Trust Act of 2011, H.R. 1841, 112th Congress (2011); Secure and Fortify Electronic Data Act, H.R. 2577, 112th Congress (2011).

Federal agencies have taken significant steps to improve consumer privacy as well. For its part, since issuing the preliminary staff report, the FTC has resolved seven data security cases,[20] obtained orders against Google, Facebook, and online ad networks,[21] and challenged practices that violate sector-specific privacy laws like the Fair Credit Reporting Act ("FCRA") and COPPA.[22] The Commission has also proposed amendments to the COPPA Rule to address changes in technology. The comment period on the Proposed Rulemaking ran through December 23, 2011, and the Commission is currently reviewing the comments received.[23] Additionally, the Commission has hosted public workshops on discrete privacy issues such as child identity theft and the use of facial recognition technology.

Other federal agencies have also begun examining privacy issues. In 2011, the Federal Communications Commission ("FCC") hosted a public forum to address privacy concerns associated with location-based services.[24] The Department of Health and Human Services ("HHS") hosted a forum on medical identity theft, developed a model privacy notice for personal health records,[25] and is developing legislative recommendations on privacy and security for such personal health records. In addition, HHS recently launched an initiative to identify privacy and security best practices for using mobile devices in health care settings.[26]

---

20 *See In the Matter of Upromise, Inc.*, FTC File No. 102 3116 (Jan. 18, 2012) (proposed consent order), *available at* http://www.ftc.gov/os/caselist/1023116/index.shtm; *In the Matter of ACRAnet, Inc.*, FTC Docket No. C-4331 (Aug. 17, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/0923088/index.shtm; *In the Matter of SettlementOne Credit Corp.*, FTC Docket No. C-4330 (Aug. 17, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/0823208/index.shtm; *In the Matter of Ceridian Corp.*, FTC Docket No. C-4325 (June 8, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023160/index.shtm; *In the Matter of Lookout Servs., Inc.*, FTC Docket No. C-4326 (June 15, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023076/index.shtm; *In the Matter of Twitter, Inc.*, FTC Docket No. C-4316 (Mar. 2, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/0923093/index.shtm; *In the Matter of Fajilan & Assocs., Inc.*, FTC Docket No. C-4332 (Aug. 17, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/0923089/index.shtm.

21 *See In the Matter of Google, Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023136/index.shtm (requiring company to implement privacy program subject to independent third-party audit); *In the Matter of Facebook, Inc.*, FTC File No. 092 3184 (Nov. 29, 2011) (proposed consent order), *available at* http://www.ftc.gov/os/caselist/0923184/index.shtm (requiring company to implement privacy program subject to independent third-party audit); *In the Matter of Chitika, Inc.*, FTC Docket No. C-4324 (June 7, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023087/index.shtm (requiring company's behavioral advertising opt out to last for five years); *In the Matter of ScanScout, Inc.*, FTC Docket No. C-4344 (Dec. 14, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023185/index.shtm (requiring company to improve disclosure of its data collection practices and offer consumers a user-friendly opt out mechanism).

22 Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*; COPPA Rule, 16 C.F.R. Part 312; *see also, e.g., United States v. W3 Innovations, LLC*, No. CV-11-03958 (N.D. Cal. Sept. 8, 2011) (COPPA consent decree); *United States v. Teletrack, Inc.*, No. 1 11-CV-2060 (N.D. Ga. filed June 24, 2011) (FCRA consent decree); *United States v. Playdom, Inc.*, No. SACV-11-00724-AG (ANx) (C.D. Cal. May 24, 2011) (COPPA consent decree).

23 *See* Press Release, FTC Extends Deadline for Comments on Proposed Amendments to the Children's Online Privacy Protection Rule Until December 23 (Nov. 18, 2011), *available at* http://www.ftc.gov/opa/2011/11/coppa.shtm.

24 *See* FCC Workshop, *Helping Consumers Harness the Potential of Location-Based Services* (June 28, 2011), *available at* http://www.fcc.gov/events/location-based-services-forum.

25 *See* The Office of the National Coordinator for Health Information Technology, Personal Health Record (PHR) Model Privacy Notice, http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__draft_phr_model_notice/1176.

26 *See* HHS Workshop, *Mobile Devices Roundtable: Safeguarding Health Information*, *available at* http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__mobile_devices_roundtable/3815.

The private sector has taken steps to enhance user privacy and security as well. For example, Google and Facebook have improved authentication mechanisms to give users stronger protection against compromised passwords.[27] Also, privacy-enhancing technologies such as the HTTPS Everywhere browser add-on have given users additional tools to encrypt their information in transit.[28] On the mobile front, the Mobile Marketing Association released its Mobile Application Privacy Policy.[29] This document provides guidance on privacy principles for application ("app") developers and discusses how to inform consumers about the collection and use of their data. Despite these developments, as explained below, industry still has more work to do to promote consumer privacy.

III. MAIN THEMES FROM COMMENTERS

The more than 450 comments filed in response to the preliminary staff report addressed three overarching issues: how privacy harms should be articulated; the value of global interoperability of different privacy regimes; and the desirability of baseline privacy legislation to augment self-regulatory efforts. Those comments, and the Commission's analysis, are discussed below.

A. ARTICULATION OF PRIVACY HARMS

There was broad consensus among commenters that consumers need basic privacy protections for their personal information. This is true particularly in light of the complexity of the current personal data ecosystem. Some commenters also stated that the Commission should recognize a broader set of privacy harms than those involving physical and economic injury.[30] For example, one commenter cited complaints from consumers who had been surreptitiously tracked and targeted with prescription drug offers and other health-related materials regarding sensitive medical conditions.[31] what shald be wrong?

At the same time, some commenters questioned whether the costs of broader privacy protections were justified by the anticipated benefits.[32] Relatedly, many commenters raised concerns about how wider privacy protections would affect innovation and the ability to offer consumers beneficial new products and services.[33]

---

27 *See Advanced Sign-In Security For Your Google Account*, Google Official Blog (Feb. 10, 2011, 11:30 AM), http://googleblog.blogspot.com/2011/02/advanced-sign-in-security-for-your.html#!/2011/02/advanced-sign-in-security-for-your.html; Andrew Song, *Introducing Login Approvals*, Facebook Blog (May 12, 2011, 9:58 AM), http://www.facebook.com/note.php?note_id=10150172618258920.

28 *See HTTPS Everywhere*, Electronic Frontier Foundation, https://www.eff.org/https-everywhere.

29 *See* Press Release, Mobile Marketing Association, Mobile Marketing Association Releases Final Privacy Policy Guidelines for Mobile Apps (Jan. 25, 2012), *available at* http://mmaglobal.com/news/mobile-marketing-association -releases-final-privacy-policy-guidelines-mobile-apps.

30 *See Comment of TRUSTe*, cmt. #00450, at 3; *Comment of Berlin Commissioner for Data Protection & Freedom of Information*, cmt. #00484, at 1.

31 *See Comment of Patient Privacy Rights*, cmt. #00470, at 2.

32 *See Comment of Technology Policy Institute*, cmt. #00301, at 5-8; *Comment of Experian*, cmt. #00398, at 9-11; *Comment of Global Privacy Alliance*, cmt. #00367, at 6-7.

33 *See Comment of Facebook, Inc.*, cmt. #00413, at 1-2, 7-8; *Comment of Google, Inc.*, cmt. #00417, at 4; *Comment of Global Privacy Alliance*, cmt. #00367, at 16.

these would be a fun read!

The Commission agrees that the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data. These harms may include the unexpected revelation of previously private information, including both sensitive information (*e.g.*, health information, precise geolocation information) and less sensitive information (*e.g.*, purchase history, employment history) to unauthorized third parties.[34] As one example, in the Commission's case against Google, the complaint alleged that Google used the information of consumers who signed up for Gmail to populate a new social network, Google Buzz.[35] The creation of that social network in some cases revealed previously private information about Gmail users' most frequent email contacts. Similarly, the Commission's complaint against Facebook alleged that Facebook's sharing of users' personal information beyond their privacy settings was harmful.[36] Like these enforcement actions, a privacy framework should address practices that unexpectedly reveal previously private information even absent physical or financial harm, or unwarranted intrusions.[37]

In terms of weighing costs and benefits, although it recognizes that imposing new privacy protections will not be costless, the Commission believes doing so not only will help consumers but also will benefit businesses by building consumer trust in the marketplace. Businesses frequently acknowledge the importance of consumer trust to the growth of digital commerce[38] and surveys support this view. For

---

34 One former FTC Chairman, in analyzing a spyware case, emphasized that consumers should have control over what is on their computers. Chairman Majoras issued the following statement in connection with the Commission's settlement against Sony BMG resolving claims about the company's installation of invasive tracking software: "Consumers' computers belong to them, and companies must adequately disclose unexpected limitations on the customary use of their products so consumers can make informed decisions regarding whether to purchase and install that content." Press Release, FTC, Sony BMG Settles FTC Charges (Jan. 30, 2007), *available at* http://www.ftc.gov/opa/2007/01/sony.shtm; *see also* Walt Mossberg, *Despite Others' Claims, Tracking Cookies Fit My Spyware Definition*, AllThingsD (July 14, 2005, 12:01 AM), http://allthingsd.com/20050714/tracking-cookies/ ("Suppose you bought a TV set that included a component to track what you watched, and then reported that data back to a company that used or sold it for advertising purposes. Only nobody told you the tracking technology was there or asked your permission to use it. You would likely be outraged at this violation of privacy. Yet that kind of Big Brother intrusion goes on everyday on the Internet . . . [with tracking cookies].").

35 *See In re Google Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023136/110330googlebuzzcompt.pdf.

36 *See In re Facebook, Inc.*, FTC File No. 092 3184 (Nov. 29, 2011) (proposed consent order), *available at* http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.

37 Although the complaint against Google alleged that the company used deceptive tactics and violated its own privacy promises when it launched Google Buzz, even in the absence of such misrepresentations, revealing previously-private consumer data could cause consumer harm. *See* Press Release, FTC, FTC Charges Deceptive Privacy Practices in Google's Rollout of its Buzz Social Network (Mar. 30, 2011), *available at* http://www.ftc.gov/opa/2011/03/google.shtm (noting that in response to the Buzz launch, Google received thousands of complaints from consumers who were concerned about public disclosure of their email contacts which included, in some cases, ex-spouses, patients, students, employers, or competitors).

38 *See, e.g.*, Statement of John M. Montgomery, GroupM Interaction, *The State of Online Consumer Privacy: Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 112th Cong. (Mar. 16, 2011), *available at* http://www.iab.net/media/file/DC1DOCS1-432016-v1-John_Montgomery_-_Written_Testimony.pdf ("We at GroupM strongly believe in protecting consumer privacy. It is not only the right thing to do, but it is also good for business."); Statement of Alan Davidson, Director of Public Policy, Google Inc., *Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy: Hearing Before the S. Subcomm. on Privacy, Tech., and the Law*, 112th Cong. (May 10, 2011), *available at* http://www.judiciary.senate.gov/pdf/11-5-10%20Davidson%20Testimony.pdf ("Protecting privacy and security is essential for Internet commerce.").

example, in the online behavioral advertising area, a recent survey shows that consumers feel better about brands that give them transparency and control over advertisements.[39]

Companies offering consumers information about behavioral advertising and the tools to opt out of it have also found increased customer engagement. In its comment, Google noted that visitors to its Ads Preference Manager are far more likely to edit their interest settings and remain opted in rather than to opt out.[40] Similarly, another commenter conducted a study showing that making its customers aware of its privacy and data security principles – including restricting the sharing of customer data, increasing the transparency of data practices, and providing access to the consumer data it maintains – significantly increased customer trust in its company.[41]

In addition, some companies appear to be competing on privacy. For example, one company offers an Internet search service that it promotes as being far more privacy-sensitive than other search engines.[42] Similarly, in response to Google's decision to change its privacy policies to allow tracking of consumers across different Google products, Microsoft encouraged consumers to switch to Microsoft's more privacy-protective products and services.[43]

The privacy framework is designed to be flexible to permit and encourage innovation. Companies can implement the privacy protections of the framework in a way that is proportional to the nature, sensitivity, and amount of data collected as well as to the size of the business at issue. For example, the framework does not include rigid provisions such as specific disclosures or mandatory data retention and destruction periods. And, as discussed below, the framework streamlines communications for businesses and consumers alike by requiring consumer choice mechanisms only for data practices that are inconsistent with the context of a particular transaction or the business relationship with the consumer.[44]

B. GLOBAL INTEROPERABILITY

Reflecting differing legal, policy, and constitutional regimes, privacy frameworks around the world vary considerably. Many commenters cited the value to both consumers and businesses of promoting more consistent and interoperable approaches to protecting consumer privacy internationally. These commenters stated that consistency between different privacy regimes reduces companies' costs, promotes international competitiveness, and increases compliance with privacy standards.[45]

---

39 *See RESEARCH: Consumers Feel Better About Brands That Give Them Transparency and Control Over Ads*, Evidon Blog (Nov. 10, 2010), http://blog.evidon.com/tag/better-advertising ("when advertisers empower consumers with information and control over the ads they receive, a majority feels more positive toward those brands, and 36% even become more likely to purchase from those brands").

40 *See Comment of Google Inc.*, cmt. #00417, at 4.

41 *See Comment of Intuit, Inc.*, cmt. #00348, at 6-8 ("The more transparent (meaning open, simple and clear) the company is, the more customer trust increases. . . .").

42 *See* DuckDuckGo, Privacy Policy, https://duckduckgo.com/privacy.html.

43 *See* Frank X. Shaw, *Gone Google? Got Concerns? We Have Alternatives*, The Official Microsoft Blog (Feb. 1, 2012, 2:00 AM), http://blogs.technet.com/b/microsoft_blog/archive/2012/02/01/gone-google-got-concerns-we-have-alternatives.aspx.

44 See *infra* at Section IV.C.1.a.

45 *See Comment of AT&T Inc.*, cmt. #00420, at 12-13; *Comment of IBM*, cmt. #00433, at 2; *see also Comment of General Electric*, cmt. #00392, at 3 (encouraging international harmonization).

The Commission agrees there is value in greater interoperability among data privacy regimes as consumer data is increasingly transferred around the world. Meaningful protection for such data requires convergence on core principles, an ability of legal regimes to work together, and enhanced cross-border enforcement cooperation. Such interoperability is better for consumers, whose data will be subject to more consistent protection wherever it travels, and more efficient for businesses by reducing the burdens of compliance with differing, and sometimes conflicting, rules. In short, as the Administration White Paper notes, global interoperability "will provide more consistent protections for consumers and lower compliance burdens for companies."[46]

Efforts underway around the world to re-examine current approaches to protecting consumer privacy indicate an interest in convergence on overarching principles and a desire to develop greater interoperability. For example, the Commission's privacy framework is consistent with the nine privacy principles set forth in the 2004 Asia-Pacific Economic Cooperation ("APEC") Privacy Framework. Those principles form the basis for ongoing APEC work to implement a cross-border privacy rules system to facilitate data transfers among the 21 APEC member economies, including the United States.[47] In 2011, the Organization for Economic Cooperation and Development ("OECD") issued a report re-examining its seminal 1980 Privacy Guidelines in light of technological changes over the past thirty years.[48] Further, the European Commission has recently proposed legislation updating its 1995 data protection directive and proposed an overhaul of the European Union approach that focuses on many of the issues raised elsewhere in this report as well as issues relating to international transfers and interoperability.[49] These efforts reflect a commitment to many of the high-level principles embodied in the FTC's framework – increased transparency and consumer control, the need for privacy protections to be built into basic business practices, and the importance of accountability and enforcement. They also reflect a shared international interest in having systems that work better with each other, and are thus better for consumers.

---

46 White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, ii, Foreword (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

47 The nine principles in the APEC Privacy Framework are preventing harm, notice, collection limitations, uses of personal information, choice, integrity of personal information, security safeguards, access and correction, accountability. Businesses have developed a code of conduct based on these nine principles and will obtain third-party certification of their compliance. A network of privacy enforcement authorities from participating APEC economies, such as the FTC, will be able to take enforcement actions against companies that violate their commitments under the code of conduct. *See* Press Release, FTC, FTC Welcomes a New Privacy System for the Movement of Consumer Data Between the United States and Other Economies in the Asia-Pacific Region (Nov. 14, 2011), *available at* http://www.ftc.gov/opa/2011/11/apec.shtm).

48 *See* Organization for Economic Co-operation and Development, *The Evolving Privacy Landscape: 30 Years after the OECD Privacy Guidelines* (Apr. 2011), *available at* http://www.oecd.org/dataoecd/22/25/47683378.pdf.

49 European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

C. LEGISLATION TO AUGMENT SELF-REGULATORY EFFORTS

Numerous comments, including those from large industry stakeholders, consumer and privacy advocates, and individual consumers supported some form of baseline privacy legislation that incorporates the FIPPs.[50] Business commenters noted that legislation would help provide legal certainty,[51] serve as a key mechanism for building trust among customers,[52] and provide a way to fill gaps in existing sector-based laws.[53] Consumer and privacy advocates cited the inability of self-regulation to provide comprehensive and long-lasting protection for consumers.[54] One such commenter cited the fact that many self-regulatory initiatives that arose in response to the Commission's 2000 recommendation for privacy legislation were short-lived and failed to provide long-term privacy protections for consumers.[55]

At the same time, a number of commenters raised concerns about government action beyond providing guidance for self-regulatory programs.[56] Some cautioned the FTC about taking an approach that might impede industry's ability to innovate and develop new products and services in a rapidly changing marketplace. Others noted that a regulatory approach could lead to picking "winners and losers" among particular technologies and business models and called for a technology-neutral approach.[57] Commenters also argued that it might be impractical to craft omnibus standards or rules that would apply broadly across different business sectors.[58]

The Commission agrees that, to date, self-regulation has not gone far enough. In most areas, with the notable exception of efforts surrounding Do Not Track, there has been little self-regulation. For example, the FTC's recent survey of mobile apps marketed to children revealed that many of these apps fail to provide any disclosure about the extent to which they collect and share consumers' personal data.[59] Similarly, efforts

50 *See, e.g., Comment of eBay*, cmt. #00374, at 2; *Comment of Intel Corp.*, cmt. #00246, at 3-7; *Comment of Microsoft Corp.*, cmt. #00395, at 4; *Comment of Intuit, Inc.*, cmt. #00348, at 13-14; *Comment of Center for Democracy & Technology*, cmt. #00469, at 1, 7; *Comment of Gregory Byrd*, cmt. #00144, at 1; *Comment of Ellen Klinefelter*, cmt. #00095, at 1.

51 *See Comment of Microsoft Corp.*, cmt. #00395, at 4.

52 *See Comment of Intel Corp.*, cmt. #00246, at 3.

53 *See Comment of Intuit, Inc.*, cmt. #00348, at 13.

54 *See Comment of Electronic Privacy Information Center*, cmt. #00386, at 2; *Comment of World Privacy Forum*, cmt. #00376, at 2-3, 8-17.

55 *See Comment of World Privacy Forum*, cmt. #00376, at 2-3, 8-17.

56 *See Comment of Consumer Data Industry Ass'n*, cmt. #00363, at 4-5; *Comment of American Catalog Mailers Ass'n*, cmt. #00424, at 3; *Comment of Facebook, Inc.*, cmt. #00413, at 13-14; *Comment of Google Inc.*, cmt. #00417, at 8; *Comment of Verizon*, cmt. #00428, at 2-3, 6-7, 14-17; *Comment of Mortgage Bankers Ass'n*, cmt. #00308, at 2; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 3, 5, 7-13; *Comment of CTIA – The Wireless Ass'n*, cmt. #00375, at 15.

57 *See Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 32-37; *Comment of USTelecom*, cmt. #00411, at 5-7; *Comment of Verizon*, cmt. #00428, at 4-6; *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 5-6.

58 *See Comment of Consumer Data Industry Ass'n*, cmt. #00363, at 4-6; *see also Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 8-11; *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 13.

59 FTC Staff, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Feb. 2012), *available at* http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf; *FPF Finds Nearly Three-Quarters of Most Downloaded Mobile Apps Lack a Privacy Policy*, Future of Privacy Forum, http://www.futureofprivacy.org/2011/05/12/fpf-finds-nearly-three-quarters-of-most-downloaded-mobile-apps-lack-a-privacy-policy/.

of the data broker industry to establish self-regulatory rules concerning consumer privacy have fallen short.[60] These examples illustrate that even in some well-established markets, basic privacy concepts like transparency about the nature of companies' data practices and meaningful consumer control are absent. This absence erodes consumer trust.

There is also widespread evidence of data breaches and vulnerabilities related to consumer information.[61] Published reports indicate that some breaches may have resulted from the unintentional release of consumer data, for which companies later apologized and took action to address.[62] Other incidents involved planned releases or uses of data by companies that ultimately did not occur due to consumer and public backlash.[63] Still other incidents involved companies' failure to take reasonable precautions and resulted in FTC consent decrees. These incidents further undermine consumer trust, which is essential for business growth and innovation.[64]

The ongoing and widespread incidents of unauthorized or improper use and sharing of personal information are evidence of two points. First, companies that do not intend to undermine consumer privacy simply lack sufficiently clear standards to operate and innovate while respecting the expectations of consumers. Second, companies that do seek to cut corners on consumer privacy do not have adequate legal incentives to curtail such behavior.

To provide clear standards and appropriate incentives to ensure basic privacy protections across all industry sectors, in addition to reiterating its call for federal data security legislation,[65] the Commission calls

---

60 *See Comment of Center for Democracy & Technology*, cmt. #00469, at 2-3; *Comment of World Privacy Forum*, cmt. #00376, at 2-3. Discussed more fully *infra* at Section IV.D.2.a.

61 *See* Grant Gross, *Lawmakers Question Sony, Epsilon on Data Breaches,* PC World (June 2, 2011 3:40 PM), *available at* http://www.pcworld.com/businesscenter/article/229258/lawmakers_question_sony_epsilon_on_data_breaches.html; Dwight Silverman, *App Privacy: Who's Uploading Your Contact List?*, Houston Chronicle (Feb. 15, 2012 8:10 AM), http://blog.chron.com/techblog/2012/02/app-privacy-whos-uploading-your-contact-list/; Dan Graziano, *Like iOS apps, Android Apps Can Secretly Access Photos Thanks to Loophole,* BGR (Mar. 1, 2012 3:45 PM), http://www.bgr.com/2012/03/01/like-ios-apps-android-apps-can-also-secretly-access-photos-thanks-to-security-hole/.

62 *CEO Apologizes After Path Social App Uploads Contact Lists,* KMOV.com (Feb. 9, 2012 11:11AM), http://www.kmov.com/news/consumer/CEO-apologizes-after-Path-uploads-contact-lists--139015729.html; Daisuke Wakabayashi, *A Contrite Sony Vows Tighter Security,* Wall St. J. May 1, 2011, *available at* http://online.wsj.com/article/SB10001424052748704436004576296302384608280.html.

63 Kevin Parrish, *OnStar Changes its Mind About Tracking Vehicles,* Tom's Guide (Sept. 29, 2011 7:30 AM), http://www.tomsguide.com/us/OnStar-General-motors-Linda-Marshall-GPS-Terms-and-conditions,news-12677.html.

64 Surveys of consumer attitudes towards privacy conducted in the past year are illuminating. For example, a *USA Today*/Gallup poll indicated that a majority of the Facebook members or Google users surveyed were "very" or "somewhat concerned" about their privacy while using these services. Lymari Morales, *Google and Facebook Users Skew Young, Affluent, and Educated,* Gallup (Feb. 17, 2011), *available at* http://www.gallup.com/poll/146159/facebook-google-users-skew-young-affluent-educated.aspx.

65 The Commission has long supported federal laws requiring companies to implement reasonable security measures and to notify consumers in the event of certain security breaches. *See, e.g.*, Prepared Statement of the FTC, *Data Security: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade*, 112th Cong. (June 15, 2011), *available at* http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf; Prepared Statement of the FTC, *Protecting Social Security Numbers From Identity Theft: Hearing Before the Before the H. Comm. on Ways and Means, Subcomm. on Social Security*, 112th Cong. (April 13, 2011), *available at* http://www.ftc.gov/os/testimony/110411ssn-idtheft.pdf; FTC, *Security in Numbers, SSNs and ID Theft* (Dec. 2008), *available at* http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf; President's Identity Theft Task Force, *Identity Theft Task Force Report* (Sept. 2008), *available at* http://www.idtheft.gov/reports/IDTReport2008.pdf.

on Congress to consider enacting baseline privacy legislation that is technologically neutral and sufficiently flexible to allow companies to continue to innovate. The Commission is prepared to work with Congress and other stakeholders to craft such legislation.

In their comments, many businesses indicated that they already incorporate the FIPPS into their practices. For these companies, a legislative mandate should not impose an undue burden and indeed, will "level the playing field" by ensuring that all companies are required to incorporate these principles into their practices.

For those companies that are not already taking consumer privacy into account – either because of lack of understanding or lack of concern – legislation should provide clear rules of the road. It should also provide adequate deterrence through the availability of civil penalties and other remedies.[66] In short, legislation will provide businesses with the certainty they need to understand their obligations and the incentive to meet those obligations, while providing consumers with confidence that businesses will be required to respect their privacy. This approach will create an environment that allows businesses to continue to innovate and consumers to embrace those innovations without sacrificing their privacy.[67] The Commission is prepared to work with Congress and other stakeholders to formulate baseline privacy legislation.

While Congress considers such legislation, the Commission urges industry to accelerate the pace of its self-regulatory measures to implement the Commission's final privacy framework. Over the course of the next year, Commission staff will promote the framework's implementation by focusing its policymaking efforts on five main action items, which are highlighted here and discussed further throughout the report.

- **Do Not Track:** As discussed above, industry has made significant progress in implementing Do Not Track. The browser vendors have developed tools that consumers can use to signal that they do not want to be tracked; the DAA has developed its own icon-based tool and has committed to honor the browser tools; and the W3C has made substantial progress in creating an international standard for Do Not Track. However, the work is not done. The Commission will work with these groups to complete implementation of an easy-to use, persistent, and effective Do Not Track system.
- **Mobile:** The Commission calls on companies providing mobile services to work toward improved privacy protections, including the development of short, meaningful disclosures. To this end, FTC staff has initiated a project to update its business guidance about online advertising disclosures.[68] As part of this project, staff will host a workshop on May 30, 2012 and will address, among other issues, mobile privacy disclosures and how these disclosures can be short, effective, and accessible to

66 Former FTC Chairman Casper "Cap" Weinberger recognized the value of civil penalties as a deterrent to unlawful conduct. *See Hearings on H.R. 14931 and Related Bills before the Subcomm. on Commerce and Finance of the H. Comm. on Interstate and Foreign Commerce*, 91st Cong. 53, 54 (1970) (statement of FTC Chairman Caspar Weinberger); *Hearings on S. 2246, S. 3092, and S. 3201 Before the Consumer Subcomm. of the S. Comm. on Commerce*, 91st Cong. 9 (1970) (Letter from FTC Chairman Caspar W. Weinberger) (forwarding copy of House testimony).

67 With this report, the Commission is not seeking to impose civil penalties for privacy violations under the FTC Act. Rather, in the event Congress enacts privacy legislation, the Commission believes that such legislation would be more effective if the FTC were authorized to obtain civil penalties for violations.

68 *See* Press Release, FTC, FTC Seeks Input to Revising its Guidance to Businesses About Disclosures in Online Advertising (May 26, 2011), *available at* http://www.ftc.gov/opa/2011/05/dotcom.shtm.

like Android style permissions

consumers on small screens. The Commission hopes that the workshop will spur further industry self-regulation in this area.

- **Data Brokers:** To address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information, the Commission supports targeted legislation – similar to that contained in several of the data security bills introduced in the 112th Congress – that would provide consumers with access to information about them held by a data broker.[69] To further increase transparency, the Commission calls on data brokers that compile data for marketing purposes to explore creating a centralized website where data brokers could (1) identify themselves to consumers and describe how they collect and use consumer data and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain.
- **Large Platform Providers:** To the extent that large platforms, such as Internet Service Providers ("ISPs"), operating systems, browsers, and social media, seek to comprehensively track consumers' online activities, it raises heightened privacy concerns. To further explore privacy and other issues related to this type of comprehensive tracking, FTC staff intends to host a public workshop in the second half of 2012.
- **Promoting enforceable self-regulatory codes:** The Department of Commerce, with the support of key industry stakeholders, is undertaking a project to facilitate the development of sector-specific codes of conduct. FTC staff will participate in that project. To the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work. The Commission will also continue to enforce the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join.

69 *See* Data Accountability and Trust Act, H.R. 1707, 112th Congress (2011); Data Accountability and Trust Act of 2011, H.R. 1841, 112th Congress (2011); Data Security and Breach Notification Act of 2011, S. 1207, 112th Congress (2011).

IV. PRIVACY FRAMEWORK

In addition to the general comments described above, the Commission received significant comments on the scope of the proposed framework and each individual element. Those comments, as well as several clarifications and refinements based on the Commission's analysis of the issues raised, are discussed below.

A. SCOPE

Proposed Scope: The framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device.

A variety of commenters addressed the framework's proposed scope. Some of these commenters supported an expansive reach while others proposed limiting the framework's application to particular types of entities and carving out certain categories of businesses. Commenters also called for further clarification regarding the type of data the framework covers and staff's proposed "reasonably linked" standard.

1. COMPANIES SHOULD COMPLY WITH THE FRAMEWORK UNLESS THEY HANDLE ONLY LIMITED AMOUNTS OF NON-SENSITIVE DATA THAT IS NOT SHARED WITH THIRD PARTIES.

Numerous commenters addressed whether the framework should apply to entities that collect, maintain, or use limited amounts of data. Several companies argued that the burden the framework could impose on small businesses outweighed the reduced risk of harm from the collection and use of limited amounts of non-sensitive consumer data.[70] These commenters proposed that the framework not apply to entities that collect or use non-sensitive data from fewer than 5,000 individuals a year where the data is used for limited purposes, such as internal operations and first-party marketing.[71] As additional support for this position, these commenters noted that proposed privacy legislation introduced in the 111th Congress contained an exclusion to this effect.[72]

Although one consumer and privacy organization supported a similar exclusion,[73] others expressed concern about exempting, *per se*, any types of businesses or quantities of data from the framework's scope.[74] These commenters pointed to the possibility that excluded companies would sell the data to third parties, such as advertising networks or data brokers.

The Commission agrees that the first-party collection and use of non-sensitive data (*e.g.*, data that is not a Social Security number or financial, health, children's, or geolocation information) creates fewer privacy

70 *See Comment of eBay, Inc.*, cmt. #00374, at 3; *Comment of Microsoft Corp.*, cmt. #00395, at 4.

71 *Id.*

72 *See* BEST PRACTICES ACT, H.R. 5777, 111th Congress (2010); Staff Discussion Draft, H.R. __ , 111th Congress (2010), *available at* http://www.nciss.org/legislation/BoucherStearnsprivacydiscussiondraft.pdf.

73 *Comment of the Center for Democracy & Technology*, cmt. #00469, at 1.

74 *See Comment of the Electronic Frontier Foundation*, cmt. #00400, at 1; *Comment of the Consumer Federation of America*, cmt. #00358, at 2.

concerns than practices that involve sensitive data or sharing with third parties.[75] Accordingly, entities that collect limited amounts of non-sensitive consumer data from under 5,000 consumers need not comply with the framework, as long as they do not share the data with third parties. For example, consider a cash-only curb-side food truck business that offers to send messages announcing when it is in a given neighborhood to consumers who provide their email addresses. As long as the food truck business does not share these email addresses with third parties, the Commission believes that it need not provide privacy disclosures to its customers. This narrow exclusion acknowledges the need for flexibility for businesses that collect limited amounts of non-sensitive information. It also recognizes that some business practices create fewer potential risks to consumer information.

2. THE FRAMEWORK SETS FORTH BEST PRACTICES AND CAN WORK IN TANDEM WITH EXISTING PRIVACY AND SECURITY STATUTES.

The proposed framework's applicability to commercial sectors that are covered by existing laws generated comments primarily from representatives of the healthcare and financial services industries. These commenters noted that statutes such as the Health Insurance Portability and Accountability Act ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and the Gramm-Leach-Bliley Act ("GLBA") already impose privacy protections and security requirements through legal obligations on companies in these industries.[76] Accordingly, these commenters urged the Commission to avoid creating duplicative or inconsistent standards and to clarify that the proposed framework is intended to cover only those entities that are not currently covered by existing privacy and security laws. Another commenter, however, urged government to focus on fulfilling consumer privacy expectations across all sectors, noting that market evolution is blurring distinctions about who is covered by HIPAA and that consumers expect organizations to protect their personal health information, regardless of any sector-specific boundaries.[77]

The Commission recognizes the concern regarding potentially inconsistent privacy obligations and notes that, to the extent Congress enacts any of the Commission's recommendations through legislation, such legislation should not impose overlapping or duplicative requirements on conduct that is already regulated.[78] However, the framework is meant to encourage best practices and is not intended to conflict with requirements of existing laws and regulations. To the extent that components of the framework exceed, but do not conflict with existing statutory requirements, entities covered by those statutes should view the framework as best practices to promote consumer privacy. For example, it may be appropriate for financial institutions covered by GLBA to incorporate elements of privacy by design, such as collection limitations, or

75 See *infra* at Sections IV.C.1.b.(v) and IV.C.2.e.(ii), for a discussion of what constitutes sensitive data.

76 *See Comment of the Confidentiality Coalition c/o the Healthcare Leadership Council*, cmt. #00349, at 1-4; *Comment of Experian*, cmt. #00398, at 8-10; *Comment of IMS Health*, cmt. #00380, at 2-3; *Comment of Medco Health Solutions, Inc.*, cmt. #00393, at 3; *Comment of SIFMA*, cmt. #00265, at 2-3.

77 *Comment of The Markle Foundation*, cmt. #00456, at 3-10.

78 Any baseline privacy law Congress may enact would likely consider the best way to take into account obligations under existing statutes.

to improve transparency by providing reasonable access to consumer data in a manner that does not conflict with their statutory obligations. In any event, the framework provides an important baseline for entities that are not subject to sector-specific laws like HIPAA or GLBA.[79]

3. THE FRAMEWORK APPLIES TO OFFLINE AS WELL AS ONLINE DATA.

In addressing the framework's applicability to "all commercial entities," numerous commenters discussed whether the framework should apply to both online and offline data. Diverse commenters expressed strong support for a comprehensive approach applicable to both online and offline data practices.[80] Commenters noted that as a practical matter, many companies collect both online and offline data.[81]

Commenters also listed different offline contexts in which entities collect consumer data. These include instances where a consumer interacts directly with a business, such as through the use of a retail loyalty card, or where a non-consumer facing entity, such as a data broker, obtains consumer data from an offline third-party source.[82] One commenter noted that, regardless of whether an entity collects or uses data from an online or an offline source, consumer privacy interests are equally affected.[83] To emphasize the importance of offline data protections, this commenter noted that while the behavioral advertising industry has started to implement self-regulatory measures to improve consumers' ability to control the collection and the use of their online data, in the offline context such efforts by data brokers and others have largely failed.[84]

By contrast, a financial industry organization argued that the FTC should take a more narrow approach by limiting the scope of the proposed framework in a number of respects, including its applicability to offline data collection and use.[85] This commenter stated that some harms in the online context may not exist offline and raised concern about the framework's unintended consequences. For example, the commenter cited the significant costs that a requirement to provide consumers with access to data collected about them

79 There may be entities that operate within covered sectors but that nevertheless fall outside of a specific law's scope. For instance, a number of entities that collect health information are not subject to HIPAA. These entities include providers of personal health records – online portfolios that consumers can use to store and keep track of their medical information. In 2009, Congress passed the HITECH Act, which required HHS, in consultation with the FTC, to develop legislative recommendations on privacy and security requirements that should apply to these providers of personal health records and related entities. Health Information Technology ("HITECH") Provisions of American Recovery and Reinvestment Act of 2009, Title XIII, Subtitle D (Pub. L. 111-5, 123 Stat. 115, codified in relevant part at 42 U.S.C. §§ 17937 and 17954). FTC staff is consulting with HHS on this project.

80 *See Comment of the Center for Democracy & Technology*, cmt. #00469, at 2; *Comment of the Computer & Communications Industry Ass'n*, cmt. #00434, at 14; *Comment of Consumers Union*, cmt. #00362, at 4-5; *Comment of the Department of Veterans Affairs*, cmt. #00479, at 3; *Comment of Experian*, cmt. #00398, at 1; *Comment of Google Inc.*, cmt. #00417, at 7; *Comment of Microsoft Corp.*, cmt. #00395, at 4.

81 *See Comment of the Department of Veterans Affairs*, cmt. #00479, at 3 n.7; *Comment of the Computer & Communications Industry Ass'n*, cmt. #00434, at 14; *Comment of Consumers Union*, cmt. #00362, at 1.

82 *See Comment of the Department of Veterans Affairs*, cmt. #00479, at 3 n.7; *Comment of the Computer & Communications Industry Ass'n*, cmt. #00434, at 14.

83 *Comment of Center for Democracy & Technology*, cmt. #00469, at 2.

84 *Comment of Center for Democracy & Technology*, cmt. #00469, at 2-3.

85 *Comment of the Financial Services Forum*, cmt. #00381, at 8-9.

would impose on companies that collect and maintain data in paper rather than electronic form. Another commenter cited the costs of providing privacy disclosures and choices in an offline environment.[86]

The Commission notes that consumers face a landscape of virtually ubiquitous collection of their data. Whether such collection occurs online or offline does not alter the consumer's privacy interest in his or her data. For example, the sale of a consumer profile containing the consumer's purchase history from a brick-and-mortar pharmacy or a bookstore would not implicate fewer privacy concerns simply because the profile contains purchases from an offline retailer rather than from an online merchant. Accordingly, the framework applies in all commercial contexts, both online and offline.

4. THE FRAMEWORK APPLIES TO DATA THAT IS REASONABLY LINKABLE TO A SPECIFIC CONSUMER, COMPUTER, OR DEVICE.

The scope issue that generated the most comments, from a wide range of interested parties, was the proposed framework's applicability to "consumer data that can be reasonably linked to a specific consumer, computer, or other device."

A number of commenters supported the proposed framework's application to data that, while not traditionally considered personally identifiable, is linkable to a consumer or device. In particular, several consumer and privacy groups elaborated on the privacy concerns associated with supposedly anonymous data and discussed the decreasing relevance of the personally identifiable information ("PII") label.[87] These commenters pointed to studies demonstrating consumers' objections to being tracked, regardless of whether the tracker explicitly learns a consumer name, and the potential for harm, such as discriminatory pricing based on online browsing history, even without the use of PII.[88]

Similarly, the commenters noted, the ability to re-identify "anonymous" data supports the proposed framework's application to data that can be reasonably linked to a consumer or device. They pointed to incidents, identified in the preliminary staff report, in which individuals were re-identified from publicly released data sets that did not contain PII.[89] One commenter pointed out that certain industries extensively

---

86 *Comment of National Retail Federation*, cmt. #00419, at 6 (urging FTC to limit privacy framework to online collection of consumer data because applying it to offline collection would be onerous for businesses and consumers).

87 *See Comment of the Center for Democracy & Technology*, cmt. #00469, at 3; *Comment of Consumers Union*, cmt. #00362, at 4-5. In addition, in their comments both AT&T and Mozilla recognized that the distinction between PII and non-PII is blurring. *Comment of AT&T Inc.*, cmt. #00420, at 13; *Comment of Mozilla*, cmt. #00480, at 6.

88 *Comment of Center for Democracy & Technology*, cmt. #00469, at 3 (citing Edward C. Baig, *Internet Users Say, Don't Track Me*, USA TODAY, Dec. 14, 2010, *available at* http://www.usatoday.com/money/advertising/2010-12-14-donottrackpoll14_ST_N.htm); Scott Cleland, *Americans Want Online Privacy – Per New Zogby Poll*, THE PRECURSOR BLOG (June 8, 2010), http://www.precursorblog.com/content/americans-want-online-privacy-new-zogby-poll); *Comment of Consumers Union*, cmt. #00362, at 4 (discussing the potential for discriminatory pricing (citing Annie Lowery, *How Online Retailers Stay a Step Ahead of Comparison Shoppers*, WASH. POST, Dec. 12, 2010, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/12/11/AR2010121102435.html)).

89 For a brief discussion of such incidents, see FTC, *Protecting Consumer Privacy in an Era of Rapid Change, A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, at 38 (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

mine data for marketing purposes and that re-identification is a commercial enterprise.[90] This adds to the likelihood of data re-identification.

Some industry commenters also recognized consumers' privacy interest in data that goes beyond what is strictly labeled PII.[91] Drawing on the FTC's roundtables as well as the preliminary staff report, one such commenter noted the legitimate interest consumers have in controlling how companies collect and use aggregated or de-identified data, browser fingerprints,[92] and other types of non-PII.[93] Another company questioned the notion of distinguishing between PII and non-PII as a way to determine what data to protect.[94] Supporting a scaled approach rather than a bright line distinction, this commenter noted that all data derived from individuals deserves some level of protection.[95]

Other commenters representing industry opposed the proposed framework's application to non-PII that can be reasonably linked to a consumer, computer, or device.[96] These commenters asserted that the risks associated with the collection and use of data that does not contain PII are simply not the same as the risks associated with PII. They also claimed a lack of evidence demonstrating that consumers have the same privacy interest in non-PII as they do with the collection and use of PII. Instead of applying the framework to non-PII, these commenters recommended the Commission support efforts to de-identify data.

Overall, the comments reflect a general acknowledgment that the traditional distinction between PII and non-PII has blurred and that it is appropriate to more comprehensively examine data to determine the data's privacy implications.[97] However, some commenters, including some of those cited above, argued that the proposed framework's "linkability" standard is potentially too open-ended to be practical.[98] One industry organization asserted, for instance, that if given enough time and resources, any data may be linkable to an

but these are normal investigative resources

90 *Comment of Electronic Frontier Foundation*, cmt. #00400, at 4 (citing Julia Angwin & Steve Stecklow, *'Scrapers' Dig Deep for Data on Web*, WALL ST. J., Oct. 12, 2010, *available at* http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html); *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653 (2011).

91 *Comment of Mozilla*, cmt. #00480, at 4-5; *Comment of Google Inc.*, cmt. #00417, at 8.

92 The term "browser fingerprints" refers to the specific combination of characteristics – such as system fonts, software, and installed plugins – that are typically made available by a consumer's browser to any website visited. These characteristics can be used to uniquely identify computers, cell phones, or other devices. Browser fingerprinting does not rely on cookies. *See* Erik Larkin, *Browser Fingerprinting Can ID You Without Cookies*, PCWORLD, Jan. 29, 2010, *available at* http://www.pcworld.com/article/188161/browser_fingerprinting_can_id_you_without_cookies.html.

93 *Comment of Mozilla*, cmt. #00480, at 4-5 (citing FTC, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, at 36-37 (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf).

94 *Comment of Google Inc.*, cmt. #00417, at 8.

95 *Comment of Google Inc.*, cmt. #00417, at 8.

96 *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 13-14; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 13-17.

97 *See Comment of AT&T Inc.*, cmt. #00420, at 13-15; *Comment of Center for Democracy & Technology* (Feb. 18, 2011), cmt. #00469, at 3-4; *Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 3-4; *Comment of Consumers Union*, cmt. #00362, at 4-5; *Comment of Electronic Frontier Foundation*, cmt. #00400, at 1-4; *Comment of Google Inc.*, cmt. #00417, at 7-8; *Comment of Mozilla*, cmt. #00480, at 4-6; *Comment of Phorm Inc.*, cmt. #00353, at 3-4.

98 *Comment of AT&T Inc.*, cmt. #00420, at 13; Comment of *CTIA - The Wireless Ass'n*, cmt. #00375 at 3-4; *Comment of Google Inc.*, cmt. #00417, at 8; *Comment of Phorm Inc.*, cmt. #00353, at 4.

individual.[99] In addition, commenters stated that requiring the same level of protection for all data would undermine companies' incentive to avoid collecting data that is more easily identified or to take steps to de-identify the data they collect and use.[100] Other commenters argued that applying the framework to data that is potentially linkable could conflict with the framework's privacy by design concept, as companies could be forced to collect more information about consumers than they otherwise would in order to be able to provide those consumers with effective notice, choice, or access.[101] To address these concerns, some commenters proposed limiting the framework to data that is actually linked to a specific consumer, computer, or device.[102]

One commenter recommended that the Commission clarify that the reasonably linkable standard means non-public data that can be linked with *reasonable effort*.[103] This commenter also stated that the framework should exclude data that, through contract or by virtue of internal controls, will not be linked with a particular consumer. Taking a similar approach, another commenter suggested that the framework should apply to data that is reasonably likely to relate to an identifiable consumer.[104] This commenter also noted that a company could commit through its privacy policy that it would only maintain or use data in a de-identified form and that such a commitment would be enforceable under Section 5 of the FTC Act.[105]

The Commission believes there is sufficient support from commenters representing an array of perspectives – including consumer and privacy advocates as well as of industry representatives – for the framework's application to data that, while not yet linked to a particular consumer, computer, or device, may reasonably become so. There is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer, or device even if the individual pieces of data do not constitute PII.[106] Moreover, not only is it possible to re-identify non-PII data through various means,[107] businesses have strong incentives to actually do so.

In response to the comments, to provide greater certainty for companies that collect and use consumer data, the Commission provides additional clarification on the application of the reasonable linkability standard to describe how companies can take appropriate steps to minimize such linkability. Under the final

---

99 *Comment of GS1*, cmt. #00439, at 2.

100 *Comment of AT&T Inc.*, cmt. #00420, at 13-14; *Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 4; *Comment of Experian*, cmt. #00398, at 11; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 16.

101 *Comment of United States Council for International Business*, cmt. #00366, at 1; *Comment of Phorm Inc.*, cmt. #00353, at 3.

102 *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 4; *Comment of Yahoo! Inc.*, cmt. #00444, at 3-4; *Comment of GS1*, cmt. #00439, at 3.

103 *Comment of AT&T Inc.*, cmt. #00420, at 13.

104 *Comment of Intel Corp.*, cmt. #00246, at 9.

105 *Comment of Intel Corp.*, cmt. #00246, at 9.

106 FTC, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, 35-38 (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; *Comment of Center for Democracy & Technology*, cmt. #00469, at 3; *Comment of Statz, Inc.*, cmt. #00377, at 11-12. *See supra* note 89.

107 *See* FTC, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, 21-24, 43-45 (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P0085400behavadreport.pdf; Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. Rev. 1814, 1836-1848 (2011).

framework, a company's data would not be reasonably linkable to a particular consumer or device to the extent that the company implements three significant protections for that data.

First, the company must take reasonable measures to ensure that the data is de-identified. This means that the company must achieve a reasonable level of justified confidence that the data cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, computer, or other device. Consistent with the Commission's approach in its data security cases,[108] what qualifies as a reasonable level of justified confidence depends upon the particular circumstances, including the available methods and technologies. In addition, the nature of the data at issue and the purposes for which it will be used are also relevant. Thus, for example, whether a company publishes data externally affects whether the steps it has taken to de-identify data are considered reasonable. The standard is not an absolute one; rather, companies must take reasonable steps to ensure that data is de-identified.

Depending on the circumstances, a variety of technical approaches to de-identification may be reasonable, such as deletion or modification of data fields, the addition of sufficient "noise" to data, statistical sampling, or the use of aggregate or synthetic data.[109] The Commission encourages companies and researchers to continue innovating in the development and evaluation of new and better approaches to de-identification. FTC staff will continue to monitor and assess the state of the art in de-identification.

Second, a company must publicly commit to maintain and use the data in a de-identified fashion, and not to attempt to re-identify the data. Thus, if a company does take steps to re-identify such data, its conduct could be actionable under Section 5 of the FTC Act.

Third, if a company makes such de-identified data available to other companies – whether service providers or other third parties – it should contractually prohibit such entities from attempting to re-identify the data. The company that transfers or otherwise makes the data available should exercise reasonable oversight to monitor compliance with these contractual provisions and take appropriate steps to address contractual violations.[110]

FTC staff's letter closing its investigation of Netflix, arising from the company's plan to release purportedly anonymous consumer data to improve its movie recommendation algorithm, provides a good illustration of these concepts. In response to the privacy concerns that FTC staff and others raised, Netflix revised its initial plan to publicly release the data. The company agreed to narrow any such release of data to certain researchers. The letter details Netflix's commitment to implement a number of "operational

108 The Commission's approach in data security cases is a flexible one. Where a company has offered assurances to consumers that it has implemented reasonable security measures, the Commission assesses the reasonableness based, among other things, on the sensitivity of the information collected, the measures the company has implemented to protect such information, and whether the company has taken action to address and prevent well-known and easily addressable security vulnerabilities.

109 *See, e.g.*, Cynthia Dwork, *A Firm Foundation for Private Data Analysis*, 54 COMM. OF THE ACM 86-95 (2011), *available at* http://research.microsoft.com/pubs/116123/dwork_cacm.pdf, and references cited therein.

110 *See In the Matter of Superior Mortg. Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005), *available at*, http://www.ftc.gov/os/caselist/0523136/0523136.shtm (alleging a violation of the GLB Safeguards Rule for, among other things, a failure to ensure that service providers were providing appropriate security for customer information and addressing known security risks in a timely manner).

safeguards to prevent the data from being used to re-identify consumers."[111] If it chose to share such data with third parties, Netflix stated that it would limit access "only to researchers who contractually agree to specific limitations on its use."[112] actually that might not be all that bad...

Accordingly, as long as (1) a given data set is not reasonably identifiable, (2) the company publicly commits not to re-identify it, and (3) the company requires any downstream users of the data to keep it in de-identified form, that data will fall outside the scope of the framework.[113]

This clarification of the framework's reasonable linkability standard is designed to help address the concern that the standard is overly broad. Further, the clarification gives companies an incentive to collect and use data in a form that makes it less likely the data will be linked to a particular consumer or device, thereby promoting privacy. Additionally, by calling for companies to publicly commit to the steps they take, the framework promotes accountability.[114]

Consistent with the discussion above, the Commission restates the framework's scope as follows.

> **Final Scope:** The framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device, unless the entity collects only non-sensitive data from fewer than 5,000 consumers per year and does not share the data with third parties.

B. PRIVACY BY DESIGN

> **Baseline Principle:** Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services.

The preliminary staff report called on companies to promote consumer privacy throughout their organizations and at every stage of the development of their products and services. Although many companies already incorporate substantive and procedural privacy protections into their business practices, industry should implement privacy by design more systematically. A number of commenters, including those representing industry, supported staff's call that companies "build in" privacy, with several of these commenters citing to the broad international recognition and adoption of privacy by design.[115] The Commission is encouraged to see broad support for this concept, particularly in light of the increasingly global nature of data transfers.

---

111 Letter from Maneesha Mithal, Assoc. Dir., Div. of Privacy & Identity Prot., FTC, to Reed Freeman, Morrison & Foerster LLP, Counsel for Netflix, 2 (Mar. 12, 2010), *available at* http://www.ftc.gov/os/closings/100312netflixletter.pdf (closing letter).

112 *Id.*

113 To the extent that a company maintains and uses both data that is identifiable and data that it has taken steps to de-identify as outlined here, the company should silo the data separately.

114 A company that violates its policy against re-identifying data could be subject to liability under the FTC Act or other laws.

115 *Comment of Office of the Information and Privacy Commissioner of Ontario*, cmt. #00239, at 2-3; *Comment of Intel Corp.*, cmt. #00246, at 12-13; *Comment of CNIL*, cmt. #00298, at 2-3.

In calling for privacy by design, staff advocated for the implementation of substantive privacy protections – such as data security, limitations on data collection and retention, and data accuracy – as well as procedural safeguards aimed at integrating the substantive principles into a company's everyday business operations. By shifting burdens away from consumers and placing obligations on businesses to treat consumer data in a responsible manner, these principles should afford consumers basic privacy protections without forcing them to read long, incomprehensible privacy notices to learn and make choices about a company's privacy practices. Although the Commission has not changed the proposed "privacy by design" principles, it responds to a number of comments, as discussed below.

1. THE SUBSTANTIVE PRINCIPLES: DATA SECURITY, REASONABLE COLLECTION LIMITS, SOUND RETENTION PRACTICES, AND DATA ACCURACY.

Proposed Principle: Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention practices, and data accuracy.

a. Should Additional Substantive Principles Be Identified?

Responding to a question about whether the final framework should identify additional substantive protections, several commenters suggested incorporating the additional principles articulated in the 1980 OECD Privacy Guidelines.[116] One commenter also proposed adding the "right to be forgotten," which would allow consumers to withdraw data posted online about themselves at any point.[117] This concept has gained importance as people post more information about themselves online without fully appreciating the implications of such data sharing or the persistence of online data over time.[118] In supporting an expansive view of privacy by design, a consumer advocacy group noted that the individual elements and principles of the proposed framework should work together holistically.[119]

In response, the Commission notes that the framework already embodies all the concepts in the 1980 OECD privacy guidelines, although with some updates and changes in emphasis. For example, privacy by design includes the collection limitation, data quality, and security principles. Additionally, the framework's simplified choice and transparency components, discussed below, encompass the OECD principles of purpose specification, use limitation, individual participation, and openness. The framework also adopts the

116 *Comment of CNIL*, cmt. #00298, at 2; *Comment of the Information Commissioner's Office of the UK*, cmt. #00249, at 2; *Comment of World Privacy Forum*, cmt. #00369, at 7; *Comment of Intel Corp.*, cmt. #00246, at 4; *see also* Organisation for Economic Co-operation & Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Sept. 1980), *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html (these principles include purpose specification, individual participation, accountability, and principles to govern cross-border data transfers). Another commenter called for baseline legislation based on the Fair Information Practice Principles and the principles outlined in the 1974 Privacy Act. *Comment of Electronic Privacy Information Center*, cmt. #00386, at 17-20.

117 *Comment of CNIL*, cmt. #00298, at 3.

118 The concept of the "right to be forgotten," and its importance to young consumers, is discussed in more detail below in the Transparency Section, *infra* at Section IV.D.2.b.

119 *Comment of Consumers Union*, cmt. #00362, at 1-2, 5-9, 18-19.

OECD principle that companies must be accountable for their privacy practices. Specifically, the framework calls on companies to implement procedures – such as designating a person responsible for privacy, training employees, and ensuring adequate oversight of third parties – to help ensure that they are implementing appropriate substantive privacy protections. The framework also calls on industry to increase efforts to educate consumers about the commercial collection and use of their data and the available privacy tools. In addition, there are aspects of the proposed "right to be forgotten" in the final framework, which calls on companies to (1) delete consumer data that they no longer need and (2) allow consumers to access their data and in appropriate cases suppress or delete it.[120]

All of the principles articulated in the preliminary staff report are intended to work together to shift the burden for protecting privacy away from consumers and to encourage companies to make strong privacy protections the default. Reasonable collection limits and data disposal policies work in tandem with streamlined notices and improved consumer choice mechanisms. Together, they function to provide substantive protections by placing reasonable limits on the collection, use, and retention of consumer data to more closely align with consumer expectations, while also raising consumer awareness about the nature and extent of data collection, use, and third-party sharing, and the choices available to them.

b. Data Security: Companies Must Provide Reasonable Security for Consumer Data.

It is well settled that companies must provide reasonable security for consumer data. The Commission has a long history of enforcing data security obligations under Section 5 of the FTC Act, the FCRA and the GLBA. Since 2001, the FTC has brought 36 cases under these laws, charging that businesses failed to appropriately protect consumers' personal information. Since issuance of the preliminary staff report alone, the Commission has resolved seven data security actions against resellers of sensitive consumer report information, service providers that process employee data, a college savings program, and a social media service.[121] In addition to the federal laws the FTC enforces, companies are subject to a variety of

120 *See In the Matter of Facebook, Inc.*, FTC File No. 092 3184 (Nov. 29, 2011) (proposed consent order), *available at* http://www.ftc.gov/os/caselist/0923184/index.shtm (requiring Facebook to make inaccessible within thirty days data that a user deletes); *see also* Do Not Track Kids Act of 2011, H.R. 1895, 112th Cong. (2011).

121 *In the Matter of Upromise, Inc.*, FTC File No. 102 3116 (Jan. 18, 2012) (proposed consent order), *available at* http://www.ftc.gov/os/caselist/1023116/index.shtm; *In the Matter of ACRAnet, Inc.*, FTC Docket No. C-4331(Aug. 17, 2011) (consent order), *available at* http://ftc.gov/os/caselist/0923088/index.shtm; *In the Matter of Fajilan & Assocs., Inc.*, FTC Docket No. C-4332 (Aug. 17, 2011) (consent order), *available at* http://ftc.gov/os/caselist/0923089/index.shtm; *In the Matter of SettlementOne Credit Corp.*, FTC Docket No. C-4330 (Aug. 17, 2011) (consent order), *available at* http://ftc.gov/os/caselist/0823208/index.shtm; *In the Matter of Lookout Servs., Inc.*, FTC Docket No. C-4326 (June 15, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/102376/index.shtm; *In the Matter of Ceridian Corp.*, FTC Docket No. C-4325 (June 8, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023160/index.shtm; *In the Matter of Twitter, Inc.*, FTC Docket No. C-4316 (Mar. 11, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/0923093/index.shtm.

other federal and state law obligations. In some industries, such as banking, federal regulators have given additional guidance on how to define reasonable security.[122]

The Commission also promotes better data security through consumer and business education. For example, the FTC sponsors OnGuard Online, a website to educate consumers about basic computer security.[123] Since the Commission issued the preliminary staff report there have been over 1.5 million unique visits to OnGuard Online and its Spanish-language counterpart Alerta en Línea. The Commission's business outreach includes general advice about data security as well as specific advice about emerging topics.[124]

The Commission also notes that the private sector has implemented a variety of initiatives in the security area, including the Payment Card Institute Data Security Standards for payment card data, the SANS Institute's security policy templates, and standards and best practices guidelines for the financial services industry provided by BITS, the technology policy division of the Financial Services Roundtable.[125] These standards can provide useful guidance on appropriate data security measures that organizations should implement for specific types of consumer data or in specific industries. The Commission further calls on industry to develop and implement best data security practices for additional industry sectors and other types of consumer data.

Because this issue is important to consumers and because businesses have existing legal and self-regulatory obligations, many individual companies have placed great emphasis and resources on maintaining reasonable security. For example, Google has cited certain security features in its products, including default SSL encryption for Gmail and security features in its Chrome browser.[126] Similarly, Mozilla has noted that

122 *See, e.g.*, Federal Financial Institutions Examination Council ("FFIEC"), *Information Society IT Examination Handbook* (July 2006), *available at* http://ithandbook.ffiec.gov/it-booklets/information-security.aspx; Letter from Richard Spillenkothen, Dir., Div. of Banking Supervision & Regulation, Bd. of Governors of the Fed. Reserve Sys., *SRO1-11: Identity Theft and Pretext Calling* (Apr. 26, 2011), *available at* http://www.federalreserve.gov/boarddocs/srletters/2001/sr0111.htm (guidance on pretexting and identity theft); Securities & Exchange Commission, *CF Disclosure Guidance: Topic No. 2, on Cybersecurity* (Oct. 13, 2011), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm; U.S. Small Business Administration, Information Security Guidance, http://www.sba.gov/content/information-security; National Institute of Standards & Technology, Computer Security Division, *Computer Security Resource Center*, *available at* http://csrc.nist.gov/groups/SMA/sbc/index.html; HHS, Health Information Privacy, *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html (guidance and educational materials for entities required to comply with the HIPPA Privacy and Security Rules); Centers from Medicare and Medicaid Services, *Educational Materials*, *available at* http://www.cms.gov/EducationMaterials/ (educational materials for HIPPA compliance).

123 FTC, OnGuard Online, http://onguardonline.gov/.

124 *See* FTC, *Protecting Personal Information: A Guide for Business* (Nov. 2011), *available at* http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business; *see generally* FTC, Bureau of Consumer Protection Business Center, Data Security Guidance, *available at* http://business.ftc.gov/privacy-and-security/data-security.

125 *See* PCI Security Standards Council, *PCI SSC Data Security Standards Overview*, *available at* https://www.pcisecuritystandards.org/security_standards/; SANS Institute, *Information Security Policy Templates*, *available at* http://www.sans.org/security-resources/policies/; BITS, *Financial Services Roundtable BITS Publications*, *available at* http://www.bits.org/publications/index.php; *see also, e.g.*, Better Business Bureau, *Security and Privacy – Made Simpler: Manageable Guidelines to help You Protect Your Customers' Security & Privacy from Identity Theft & Fraud*, *available at* http://www.bbb.org/us/storage/16/documents/SecurityPrivacyMadeSimpler.pdf; National Cyber Security Alliance, *For Business*, http://www.staysafeonline.org/for-business (guidance for small and midsize businesses); Direct Marketing Association, *Information Security: Safeguarding Personal Data in Your Care* (May 2005), *available at* http://www.the-dma.org/privacy/InfoSecData.pdf; Messaging Anti-Abuse Working Group & Anti-Phishing Working Group, *Anti-Phishing Best Practices for ISPs and Mailbox Providers* (July 2006), *available at* http://www.antiphishing.org/reports/bestpracticesforisps.pdf.

126 *Comment of Google Inc.*, cmt. #00417, at 2-3.

its cloud storage system encrypts user data using SSL communication.[127] Likewise, Twitter has implemented encryption by default for users logged into its system.[128] The Commission commends these efforts and calls on companies to continue to look for additional ways to build data security into products and services from the design stage.

Finally, the Commission reiterates its call for Congress to enact data security and breach notification legislation. To help deter violations, such legislation should authorize the Commission to seek civil penalties.

c. Reasonable Collection Limitation: Companies Should Limit Their Collection of Data.

The preliminary staff report called on companies to collect only the data they need to accomplish a specific business purpose. Many commenters expressed support for the general principle that companies should limit the information they collect from consumers.[129] Despite the broad support for the concept, however, many companies argued for a flexible approach based on concerns that allowing companies to collect data only for existing business needs would harm innovation and deny consumers new products and services.[130] One commenter cited Netflix's video recommendation feature as an example of how secondary uses of data can create consumer benefits. The commenter noted that Netflix originally collected information about subscribers' movie preferences in order to send the specific videos requested, but later used this information as the foundation for generating personalized recommendations to its subscribers.[131]

In addition, commenters raised concerns about who decides what a "specific business purpose" is.[132] For example, one purpose for collecting data is to sell it to third parties in order to monetize a service and provide it to consumers for free. Would collecting data for this purpose be a specific business purpose? If not, is the only alternative to charge consumers for the service, and would this result be better for consumers?

As an alternative to limiting collection to accomplish a "specific business purpose," many commenters advocated limiting collection to business purposes *that are clearly articulated*. This is akin to the Fair Information Practice Principle of "purpose specification," which holds that companies should specify to consumers all of the purposes for which information is collected at the time of collection. One commenter supported purpose specification statements in general categories to allow innovation and avoid making privacy policies overly complex.[133]

127 *Comment of Mozilla*, cmt. #00480, at 7.

128 *See* Chloe Albanesius, *Twitter Adds Always-On Encryption*, PC Magazine, Feb. 12, 2012, http://www.pcmag.com/article2/0,2817,2400252,00.asp.

129 *See, e.g.*, *Comment of Intel Corp.*, cmt. #00246, at 4-5, 7, 40-41; *Comment of Electronic Frontier Foundation*, cmt. #00400, at 4-6; *Comment of Center for Democracy & Technology*, cmt. #00469, at 4-5; *Comment of Electronic Privacy Information Center*, cmt. #00386, at 18.

130 *See, e.g.*, *Comment of Facebook, Inc.*, cmt. #00413, at 2, 7-8, 18; *Comment of Google Inc.*, cmt. #00417, at 4; *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 14-15; *Comment of Intuit, Inc.*, cmt. #00348, at 5, 9; *Comment of TRUSTe*, cmt. #00450, at 9.

131 *Comment of Facebook, Inc.*, cmt. #00413, at 7-8.

132 *See Comment of SAS*, cmt. #00415, at 51; *Comment of Yahoo! Inc.*, cmt. #00444, at 5.

133 *Comment of Yahoo! Inc.*, cmt. #00444, at 5.

The Commission recognizes the need for flexibility to permit innovative new uses of data that benefit consumers. At the same time, in order to protect consumer privacy, there must be some reasonable limit on the collection of consumer data. General statements in privacy policies, however, are not an appropriate tool to ensure such a limit because companies have an incentive to make vague promises that would permit them to do virtually anything with consumer data.

Accordingly, the Commission clarifies the collection limitation principle of the framework as follows: Companies should limit data collection to that which is consistent with the context of a particular transaction or the consumer's relationship with the business, or as required or specifically authorized by law.[134] For any data collection that is inconsistent with these contexts, companies should make appropriate disclosures to consumers at a relevant time and in a prominent manner – outside of a privacy policy or other legal document. This clarification of the collection limitation principle is intended to help companies assess whether their data collection is consistent with what a consumer might expect; if it is not, they should provide prominent notice and choice. (For a further discussion of this point, see *infra* Section IV.C.2.) This approach is consistent with the Administration's Consumer Privacy Bill of Rights, which includes a Respect for Context principle that limits the use of consumer data to those purposes consistent with the context in which consumers originally disclosed the data.[135]

One example of a company innovating around the concept of privacy by design through collection limitation is the Graduate Management Admission Council ("GMAC"). This entity previously collected fingerprints from individuals taking the Graduate Management Admission Test. After concerns were raised about individuals' fingerprints being cross-referenced against criminal databases, GMAC developed a system that allowed for collection of palm prints that could be used solely for test-taking purposes.[136] The palm print technology is as accurate as fingerprinting but less susceptible to "function creep" over time than the taking of fingerprints, because palm prints are not widely used as a common identifier. GMAC received a privacy innovation award for small businesses for its work in this area.

d. Sound Data Retention: Companies Should Implement Reasonable Data Retention and Disposal Policies.

Similar to the concerns raised about collection limits, many commenters expressed concern about limiting retention of consumer data, asserting that such limits would harm innovation. Trade associations and businesses requested a flexible standard for data retention to allow companies to develop new products

134 This approach mirrors the revised standard for determining whether a particular data practice warrants consumer choice (see *infra* at section IV.C.1.a.) and is consistent with a number of commenters' calls for considering the context in which a particular practice takes place. *See, e.g.*, *Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 2-4; *Comment of Consumer Data Industry Ass'n*, cmt. #00363, at 5; *Comment of TRUSTe*, cmt. #00450, at 3.

135 *See* White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, 15-19, (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. For a further discussion of this point, see *infra* at Section IV.C.1.a.

136 *See* Jay Cline, *GMAC: Navigating EU Approval for Advanced Biomterics*, Inside Privacy Blog (Oct. 15, 2010), https://www.privacyassociation.org/publications/2010_10_20_gmac_navigating_eu_approval_for_advanced_biometrics (explaining GMAC's adoption of palm print technology); *cf.* Kashmir Hill, *Why 'Privacy by Design' is the New Corporate Hotness*, Forbes, July 28, 2011, *available at* http://www.forbes.com/sites/kashmirhill/2011/07/28/why-privacy-by-design-is-the-new-corporate-hotness/.

and other uses of data that provide benefits to consumers.[137] One company raised concerns about prescriptive retention periods, arguing that retention standards instead should be based on business need, the type and location of data at issue, operational issues, and legal requirements.[138] Other commenters noted that retention limits should be sufficiently flexible to accommodate requests from law enforcement or other legitimate business purposes, such as the need of a mortgage banker to retain information about a consumer's payment history.[139] Some commenters suggested that the Commission's focus should be on data security and proper handling of consumer data, rather than on retention limits.[140]

In contrast, some consumer groups advocated specific retention periods. For example, one such commenter cited a proposal made by a consortium of consumer groups in 2009 that companies that collect data for online behavioral advertising should limit their retention of the data to three months and that companies that retained their online behavioral advertising data for only 24 hours may not need to obtain consumer consent for their data collection and use.[141] Others stated that it might be appropriate for the FTC to recommend industry-specific retention periods after a public consultation.[142]

The Commission confirms its conclusion that companies should implement reasonable restrictions on the retention of data and should dispose of it once the data has outlived the legitimate purpose for which it was collected.[143] Retention periods, however, can be flexible and scaled according to the type of relationship and use of the data; for example, there may be legitimate reasons for certain companies that have a direct relationship with customers to retain some data for an extended period of time. A mortgage company will maintain data for the life of the mortgage to ensure accurate payment tracking; an auto dealer will retain data from its customers for years to manage service records and inform its customers of new offers. These long retention periods help maintain productive customer relationships. This analysis does not, however, apply to all data collection scenarios. A number of commenters noted that online behavioral advertising data often becomes stale quickly and need not be retained long.[144] For example, a consumer researching hotels in a particular city for an upcoming vacation is unlikely to be interested in continuing to see hotel advertisements after the trip is completed. Indefinite retention of data about the consumer's interest in finding a hotel for a particular weekend serves little purpose and could result in marketers sending the consumer irrelevant advertising.

---

137 *See Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 2-4, 14; *Comment of American Catalog Mailers Ass'n*, cmt. #000424, at 5; *Comment of IBM*, cmt. #00433, at 4; *Comment of Intuit, Inc.*, cmt. #00348, at 9.

138 *Comment of Verizon*, cmt. #00428, at 10-11.

139 *See, e.g.*, *Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 14.

140 *Comment of Yahoo! Inc.*, cmt. #00444, at 6; *see also Comment of American Catalog Mailers Ass'n*, cmt. #00424, at 3-4.

141 *Comment of Consumer Federation of America*, cmt. #00358, at 4 (citing *Legislative Primer: Online Behavioral Tracking and Targeting Concerns and Solutions from the Perspective of the Center for Digital Democracy and U.S. PIRG, Consumer Federation of America, Consumers Union, Consumer Watchdog, Electronic Frontier Foundation, Privacy Lives, Privacy Rights Clearinghouse, Privacy Times, U.S. Public Interest Research group, The World Privacy Forum* (Sept. 2009), *available at* http://www.consumerfed.org/elements/www.consumerfed.org/file/OnlinePrivacyLegPrimerSEPT09.pdf).

142 *Comment of Center for Democracy & Technology*, cmt. #00469, at 6 ("Flexible approaches to data retention should not, however, give *carte blanche* to companies to maintain consumer data after it has outlived its reasonable usefulness.").

143 In the alternative, companies may consider taking steps to de-identify the data they maintain, as discussed above.

144 *See Comment of Consumers Union*, cmt. #00362, at 8.

In determining when to dispose of data, as well as limitations on collection described above, companies should also take into account the nature of the data they collect. For example, consider a company that develops an online interactive game as part of a marketing campaign directed to teens. The company should first assess whether it needs to collect the teens' data as part of the game, and if so, how it could limit the data collected, such as by allowing teens to create their own username instead of using a real name and email address. If the company decides to collect the data, it should consider disposing of it even more quickly than it would if it collected adults' data. Similarly, recognizing the sensitivity of data such as a particular consumer's real time location, companies should take special care to delete this data as soon as possible, consistent with the services they provide to consumers.

Although restrictions may be tailored to the nature of the company's business and the data at issue, companies should develop clear standards and train its employees to follow them. Trade associations and self-regulatory groups also should be more proactive in providing guidance to their members about retention and data destruction policies. Accordingly, the Commission calls on industry groups from all sectors – the online advertising industry, online publishers, mobile participants, social networks, data brokers and others – to do more to provide guidance in this area. Similarly, the Commission generally supports the exploration of efforts to develop additional mechanisms, such as the "eraser button" for social media discussed below,[145] to allow consumers to manage and, where appropriate, require companies to delete the information consumers have submitted.

e. Accuracy: Companies should maintain reasonable accuracy of consumers' data.

The preliminary staff report called on companies to take reasonable steps to ensure the accuracy of the data they collect and maintain, particularly if such data could cause significant harm or be used to deny consumers services. Similar to concerns raised about collection limits and retention periods, commenters opposed rigid accuracy standards,[146] and noted that the FCRA already imposes accuracy standards in certain contexts.[147] One commenter highlighted the challenges of providing the same levels of accuracy for non-identifiable data versus data that is identifiable.[148]

To address these challenges, some commenters stated that a sliding scale approach should be followed, particularly for marketing data. These commenters stated that marketing data is not used for eligibility purposes and that, if inaccurate, the only harm a consumer may experience is an irrelevant advertisement.[149] Providing enhanced accuracy standards for marketing data would raise additional privacy and data security concerns,[150] as additional information may need to be added to marketing databases to increase accuracy.[151]

145 See *infra* at Section IV.D.2.b.

146 *See Comment of Experian*, cmt. #00398, at 2.

147 *See Comment of SIFMA*, cmt. #00265, at 4.

148 *Comment of Phorm Inc.*, cmt. #00353, at 4.

149 *Comment of Experian*, cmt. #00398, at 11 (arguing against enhanced standards for accuracy, access, and correction for marketing data); *see also Comment of Yahoo! Inc.*, cmt. #00444, at 6-7.

150 *Id.*

151 *Cf. Comment of Yahoo! Inc.*, cmt. #00444, at 7 (arguing that it would be costly, time consuming, and contrary to privacy objectives to verify the accuracy of user registration information such as gender, age or hometown).

The Commission agrees that the best approach to improving the accuracy of the consumer data companies collect and maintain is a flexible one, scaled to the intended use and sensitivity of the information. Thus, for example, companies using data for marketing purposes need not take special measures to ensure the accuracy of the information they maintain. Companies using data to make decisions about consumers' eligibility for benefits should take much more robust measures to ensure accuracy, including allowing consumers access to the data and the opportunity to correct erroneous information.[152]

Final Principle: Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy.

2. COMPANIES SHOULD ADOPT PROCEDURAL PROTECTIONS TO IMPLEMENT THE SUBSTANTIVE PRINCIPLES.

Proposed Principle: Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.

In addition to the substantive principles articulated above, the preliminary staff report called for organizations to maintain comprehensive data management procedures, such as designating personnel responsible for employee privacy training and regularly assessing the privacy impact of specific practices, products, and services. Many commenters supported this call for accountability within an organization.[153] Commenters noted that privacy risk assessments promote accountability, and help identify and address privacy issues.[154] One commenter stated that privacy risk assessments should be an ongoing process, and findings should be used to update internal procedures.[155] The Commission agrees that companies should implement accountability mechanisms and conduct regular privacy risk assessments to ensure that privacy issues are addressed throughout an organization.

The preliminary staff report also called on companies to "consider privacy issues systemically, at all stages of the design and development of their products and services." A range of commenters supported the principle of "baking" privacy into the product development process.[156] One commenter stated that this approach of including privacy considerations in the product development process was preferable to requiring

152 See *infra* at Section IV.D.2. The Commission notes that some privacy-enhancing technologies operate by introducing deliberate "noise" into data. The data accuracy principle is not intended to rule out the appropriate use of these methods, provided that the entity using them notifies any recipients of the data that it is inaccurate.

153 *See, e.g.*, *Comment of The Centre for Information Policy Leadership at Hunton & Williams LLP*, cmt. #00360, at 2-3; *Comment of Intel Corp.*, cmt. #00246, at 6; *Comment of Office of the Information & Privacy Commissioner of Ontario*, cmt. #00239, at 3.

154 *Comment of GS1*, cmt. #00439, at 3; *Comment of Office of the Information & Privacy Commissioner of Ontario*, cmt. #00239, at 6.

155 *Comment of Office of the Information & Privacy Commissioner of Ontario*, cmt. #00239, at 7.

156 *Comment of Intel Corp.*, cmt. #00246, at 6; *Comment of United States Council for International Business*, cmt. #00366, at 2; *Comment of Consumer Federation of America*, cmt. #00358, at 3.

after-the-fact reviews.[157] Another argued that privacy concerns should be considered from the outset, but observed that such concerns should continue to be evaluated as the product, service, or feature evolves.[158]

The Commission's recent settlements with Google and Facebook illustrate how the procedural protections discussed above might work in practice.[159] In both cases, the Commission alleged that the companies deceived consumers about the level of privacy afforded to their data.

The FTC's orders will require the companies to implement a comprehensive privacy program reasonably designed to address privacy risks related to the development and management of new and existing products and services and to protect the privacy and confidentiality of "covered information," defined broadly to mean *any* information the companies collect from or about a consumer.

The privacy programs that the orders mandate must, at a minimum, contain certain controls and procedures, including: (1) the designation of personnel responsible for the privacy program; (2) a risk assessment that, at a minimum, addresses employee training and management and product design and development; (3) the implementation of controls designed to address the risks identified; (4) appropriate oversight of service providers; and (5) evaluation and adjustment of the privacy program in light of regular testing and monitoring.[160] Companies should view the comprehensive privacy programs mandated by these consent orders as a roadmap as they implement privacy by design in their own organizations.

As an additional means of implementing the substantive privacy by design protections, the preliminary staff report advocated the use of privacy-enhancing technologies ("PETs") – such as encryption and anonymization tools – and requested comment on implementation of such technologies. One commenter stressed the need for "privacy-aware design," calling for techniques such as obfuscation and cryptography to reduce the amount of identifiable consumer data collected and used for various products and services.[161] Another stressed that PETs are a better approach in this area than rigid technical mandates.[162]

The Commission agrees that a flexible, technology-neutral approach towards developing PETs is appropriate to accommodate the rapid changes in the marketplace and will also allow companies to innovate on PETs. Accordingly, the Commission calls on companies to continue to look for new ways to protect consumer privacy throughout the life cycle of their products and services, including through the development and deployment of PETs.

Finally, Commission staff requested comment on how to apply the substantive protections articulated above to companies with legacy data systems. Many commenters supported a phase-out period for legacy data systems, giving priority to systems that contain sensitive data.[163] Another commenter suggested that

157 *Comment of Intel Corp.*, cmt. #00246, at 6.

158 *Comment of Zynga Inc.*, cmt. #00459, at 2.

159 Of course, the privacy programs required by these orders may not be appropriate for all types and sizes of companies that collect and use consumer data.

160 *In the Matter of Google Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/index.shtm.

161 *Comment of Electronic Frontier Foundation*, cmt. #00400, at 5.

162 *Comment of Business Software Alliance*, cmt. #00389, at 7-9.

163 *Comment of The Centre for Information Policy Leadership at Hunton & Williams LLP*, cmt. #00360, at 3; *Comment of the Information Commissioner's Office of the UK*, cmt. #00249, at 2; *Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 14.

imposing strict access controls on legacy data systems until they can be updated would enhance privacy.[164] Although companies need to apply the various substantive privacy by design elements to their legacy data systems, the Commission recognizes that companies need a reasonable transition period to update their systems. In applying the substantive elements to their legacy systems, companies should prioritize those systems that contain sensitive data and they should appropriately limit access to all such systems until they can update them.

Final Principle: Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.

164 *Comment of Yahoo! Inc.*, cmt. #00444, at 7.

DATA COLLECTION AND DISPOSAL CASE STUDY: MOBILE

The rapid growth of the mobile marketplace illustrates the need for companies to implement reasonable limits on the collection, transfer, and use of consumer data and to set policies for disposing of collected data. The unique features of a mobile phone – which is highly personal, almost always on, and travels with the consumer – have facilitated unprecedented levels of data collection. Recent news reports have confirmed the extent of this ubiquitous data collection. Researchers announced, for example, that Apple had been collecting geolocation data through its mobile devices over time, and storing unencrypted data files containing this information on consumers' computers and mobile devices.[1] The Wall Street Journal has documented numerous companies gaining access to detailed information – such as age, gender, precise location, and the unique ID associated with a particular mobile device – that can then be used to track and predict consumer behavior.[2] Not surprisingly, consumers are concerned: for example, a recent Nielsen study found that a majority of smartphone app users worry about their privacy when it comes to sharing their location through a mobile device.[3] The Commission calls on companies to limit collection to data they need for a requested service or transaction. For example, a wallpaper app or an app that tracks stock quotes does not need to collect location information.[4]

The extensive collection of consumer information – particularly location information – through mobile devices also heightens the need for companies to implement reasonable policies for purging data.[5] Without data retention and disposal policies specifically tied to the stated business purpose for the data collection, location information could be used to build detailed profiles of consumer movements over time that could be used in ways not anticipated by consumers.[6] Location information is particularly useful for uniquely identifying (or re-identifying) individuals using disparate bits of data.[7] For example, a consumer can use a mobile application on her cell phone to "check in" at a restaurant for the purpose of finding and connecting with friends who are nearby. The same consumer might not expect the application provider to retain a history of restaurants she visited over time. If the application provider were to share that information with third parties, it could reveal a predictive pattern of the consumer's movements thereby exposing the consumer to a risk of harm such as stalking.[8] Taken together, the principles of reasonable collection limitation and disposal periods help to minimize the risks that information collected from or about consumers could be used in harmful or unexpected ways.

With respect to the particular concerns of location data in the mobile context, the Commission calls on entities involved in the mobile ecosystem to work together to establish standards that address data collection, transfer, use, and disposal, particularly for location data. To the extent that location data in particular is collected and shared with third parties, entities should work to provide consumers with more prominent notice and choices about such practices. Although some in the mobile ecosystem provide notice about the collection of geolocation data, not all companies have adequately disclosed the frequency or extent of the collection, transfer, and use of such data.

NOTES

1 *See* Jennifer Valentino-Devries, *Study: iPhone Keeps Tracking Data*, WALL ST. J., Apr. 21, 2011, *available at* http://online.wsj.com/article/SB10001424052748704570704576275323811369758.html.

2 *See, e.g.*, Robert Lee Hotz, *The Really Smart Phone*, WALL ST. J., Apr. 22, 2011, *available at* http://online.wsj.com/article/SB10001424052748704547604576263261679848814.html (describing how researchers are using mobile data to predict consumers' actions); Scott Thurm & Yukari Iwatane Kane, *Your Apps are Watching You*, WALL ST. J., Dec. 18, 2010, *available at* http://online.wsj.com/article/SB10001424052748704368004576027751867039730.html (documenting the data collection that occurs through many popular smartphone apps).

3 *Privacy Please! U.S. Smartphone App Users Concerned with Privacy When It Comes to Location*, NIELSENWIRE BLOG (Apr. 21, 2011), http://blog.nielsen.com/nielsenwire/online_mobile/privacy-please-u-s-smartphone-app-users-concerned-with-privacy-when-it-comes-to-location/; *see also* Ponemon Institute, *Smartphone Security: Survey of U.S. Consumers* 7 (Mar. 2011), *available at* http://aa-download.avg.com/filedir/other/Smartphone.pdf (reporting that 64% of consumers worry about their location being tracked when using their smartphones).

4 Similarly, the photo-sharing app Path faced widespread criticism for uploading its users' iPhone address books without their consent. *See, e.g.*, Mark Hachman, *Path Uploads Your Entire iPhone Contact List By Default*, PC MAGAZINE, Feb. 7, 2012, *available at* http://www.pcmag.com/article2/0,2817,2399970,00.asp.

5 The Commission is currently reviewing its COPPA Rule, including the application of COPPA to geolocation information. *See* FTC, Proposed Rule and Request for Public Comment, Children's Online Privacy Protection Rule, 76 Fed. Reg. 59,804 (Sept. 15, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-09-27/pdf/2011-24314.pdf.

6 *See* ACLU of Northern California, *Location-Based Services: Time for a Privacy Check-In*, 14-15 (Nov. 2010), *available at* http://dotrights.org/sites/default/files/lbs-white-paper.pdf.

7 *Comment of Electronic Frontier Foundation*, cmt. #00400, at 3.

8 *Cf. U.S. v. Jones*, 565 U.S. 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) (noting that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations").

C. SIMPLIFIED CONSUMER CHOICE

Baseline Principle: Companies should simplify consumer choice.

As detailed in the preliminary staff report and in submitted comments, many consumers face challenges in understanding the nature and extent of current commercial data practices and how to exercise available choices regarding those practices. This challenge results from a number of factors including: (1) the dramatic increase in the breadth of consumer data collection and use, made possible by an ever-increasing range of technologies and business models; (2) the ability of companies, outside of certain sector-specific laws, to collect and use data without first providing consumer choice; and (3) the inadequacy of typical privacy policies as a means to effectively communicate information about the privacy choices that are offered to consumers.

To reduce the burden on those consumers who seek greater control over their data, the proposed framework called on companies that collect and use consumer data to provide easy-to-use choice mechanisms that allow consumers to control whether their data is collected and how it is used. To ensure that choice is most effective, the report stated that a company should provide the choice mechanism at a time and in a context that is relevant to consumers – generally at the point the company collects the consumer's information. At the same time, however, in recognition of the benefits of various types of data collection and use, the proposed framework identified certain "commonly accepted" categories of commercial data practices that companies can engage in without offering consumer choice.

Staff posed a variety of questions and received numerous comments regarding the proposed framework's simplified consumer choice approach. Two trade organizations argued that the framework should identify those practices for which choice is appropriate rather than making choice the general rule, subject to exceptions for certain practices.[165] The majority of commenters, however, did not challenge the proposed framework's approach of setting consumer choice as the default.[166] Instead, these commenters focused on the practicality of staff's "commonly accepted" formulation.[167] For example, several commenters questioned whether the approach was sufficiently flexible to allow for innovation.[168] Others discussed whether specific practices should fall within the categories enumerated in the preliminary staff report.[169] In addition, numerous commenters addressed the appropriate scope of the first-party marketing category and how to

165 *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 16; *Comment of Interactive Advertising Bureau*, cmt. #00388, at 8-9.

166 Several commenters expressed support for consumer choice generally. *See, e.g.*, *Comment of Center for Democracy & Technology*, cmt. #00469, at 11-12; *Comment of Consumer Federation of America*, cmt. #00358, at 6-12. One governmental agency, for instance, expressly supported a general rule requiring consumer consent for the collection and any use of their information with only limited exceptions. *Comment of Department of Veteran Affairs*, cmt. #00479, at 5. Another commenter, supporting consumer choice, emphasized the importance of offering opportunities for choice beyond a consumer's initial transaction. *Comment of Catalog Choice*, cmt. #00473, at 10-18.

167 *Comment of Center for Democracy & Technology*, cmt. #00469, at 8-11; *Comment of Consumer Federation of America*, cmt. #00358, at 6-10.

168 *Comment of Computer and Communications Industry Ass'n*, cmt. #00434, at 16; *Comment of BlueKai*, cmt. #00397, at 3-4; *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 5-7; *U.S. Chamber of Commerce*, cmt. #00452, at 5; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 23-24; *Comment of Yahoo! Inc.*, cmt. #00444, at 9-10.

169 *Comment of Phorm Inc.*, cmt. #00353, at 5; *Comment of Verizon*, cmt. #00428, at 11-13.

define specific business models. With respect to those practices that fall outside the "commonly accepted" categories, commenters also addressed the mechanics of providing choice at the relevant time and what types of practices require enhanced choice.

Consistent with the discussion and analysis set forth below, the Commission retains the proposed framework's simplified choice model. Establishing consumer choice as a baseline requirement for companies that collect and use consumer data, while also identifying certain practices where choice is unnecessary, is an appropriately balanced model. It increases consumers' control over the collection and use of their data, preserves the ability of companies to innovate new products and services, and sets clear expectations for consumers and industry alike. In order to better foster innovation and take into account new technologies and business models, however, the Commission is providing further clarification of the framework's simplified choice concept.

1. PRACTICES THAT DO NOT REQUIRE CHOICE.

Proposed Principle: Companies do not need to provide choice before collecting and using consumers' data for commonly accepted practices, such as product fulfillment.

The preliminary staff report identified five categories of data practices that companies can engage in without offering consumer choice, because they involve data collection and use that is either obvious from the context of the transaction or sufficiently accepted or necessary for public policy reasons. The categories included: (1) product and service fulfillment; (2) internal operations; (3) fraud prevention; (4) legal compliance and public purpose; and (5) first-party marketing. In response to the comments received, the Commission revises its approach to focus on the context of the consumer's interaction with a company, as discussed below.

a. General Approach to "Commonly Accepted" Practices.

While generally supporting the concept that choice is unnecessary for certain practices, a variety of commenters addressed the issue of whether the list of "commonly accepted" practices was too broad or too narrow.[170] A number of industry commenters expressed concern that the list of practice categories was too narrow and rigid. These commenters stated that, by enumerating a list of specific practices, the proposed framework created a bright-line standard that freezes in place current practices and potentially could harm innovation and restrict the development of new business models.[171] In addition, the commenters asserted that notions of what is "commonly accepted" can change over time with the development of new ways to collect or use data. They also stated that line-drawing in this context could stigmatize business practices that fall outside of the "commonly accepted" category and place companies that engage in them at a competitive

170 *Comment of AT&T Inc.*, cmt. #00420, at 18-22; *Comment of Center for Democracy & Technology*, cmt. #00469, at 8-11; *Comment of Consumers Union*, cmt. #00362, at 9-12; *Comment of Consumer Federation of America*, cmt. #00358, at 6-10; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 23-25.

171 *Comment of Computer and Communications Industry Ass'n*, cmt. #00434, at 16; *Comment of BlueKai*, cmt. #00397, at 4; *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 6-7; *Comment of Yahoo! Inc.*, cmt. #00444, at 9-12; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 23-24.

disadvantage. To resolve these concerns, commenters called on the Commission to provide guidance on how future practices relate to the "commonly accepted" category.[172] Similarly, one commenter suggested that the practices identified in the preliminary staff report should serve as illustrative guidelines rather than an exhaustive and final list.[173]

Commenters also supported adding additional practices or clarifying that the "commonly accepted" category includes certain practices. Some industry commenters suggested, for example, expanding the concept of fraud prevention to include preventing security attacks, "phishing,"[174] and spamming or to protect intellectual property.[175] Other recommendations included adding analytical data derived from devices that are not tied to individuals, such as smart grid data used for energy conservation and geospatial data used for mapping, surveying or providing emergency services.[176] With respect to online behavioral advertising in particular, some trade associations recommended clarifying that the "commonly accepted" category of practices includes the use of IP addresses and third-party cookie data when used for purposes such as "frequency capping," "attribution measurement," and similar inventory or delivery measurements and to prevent click fraud.[177]

More generally, some commenters discussed the "repurposing" of existing consumer data to develop new products or services. For example, one company supported expanding the "internal operations" category to include the practice of product and service improvement.[178] One commenter recommended treating any uses of data that consumers would "reasonably expect under the circumstances" as commonly accepted.[179] Another noted that, whether a new use of consumer data should be considered commonly accepted would depend upon a variety of factors, including the extent to which the new use is consistent with previously defined uses.[180]

In contrast to the calls for expanding the "commonly accepted" practice categories to cover various practices, a number of consumer and privacy organizations advocated for a more restrictive approach to determining the practices that do not require consumer choice. Although agreeing that choice is not necessary for product and service fulfillment, one commenter stated that most of the other practices enumerated in the proposed framework – including internal operations, fraud prevention, and legal compliance and public purpose – were vague and required additional description. The commenter called on

172 *Comment of eBay*, cmt. #00374, at 6-7; *Comment of Phorm Inc.*, cmt. #00353, at 5.

173 *See Comment of AT&T Inc.*, cmt. #00420, at 18.

174 Phishing uses deceptive spam that appears to be coming from legitimate, well-known sources to trick consumers into divulging sensitive or personal information, such as credit card numbers, other financial data, or passwords.

175 *See Comment of Microsoft Corp.*, cmt. #00395, at 8 (security attacks, phishing schemes, and spamming); *Comment of Business Software Alliance*, cmt. #00389, at 5-6 (security access controls and user and employee authentication, cybercrime and fraud prevention and detection, protecting and enforcing intellectual property and trade secrets).

176 *See Comment of IBM*, cmt. #00433, at 5 (energy conservation); *Comment of Management Ass'n for Private Programming Surveyors*, cmt. #00205, at 2-3 (mapping, surveying or providing emergency services).

177 *See Comment of Online Publishers Ass'n*, cmt. #00315, at 5 (frequency capping, click fraud); *Comment of Interactive Advertising Bureau*, cmt. #00388, at 9 (attribution measurement).

178 *See Comment of AT&T Inc.*, cmt. #00420, at 18-19.

179 *See Comment of Microsoft Corp.*, cmt. #00395, at 8.

180 *See Comment of Future of Privacy Forum*, cmt. #00341, at 5.

the Commission to define these terms as narrowly as possible so that they would not become loopholes used to undermine consumer privacy.[181]

One privacy advocate expressed reservations about the breadth of the "internal operations" category of practices – specifically, the extent to which it could include product improvement and website analytics. This commenter stated that, if viewed broadly, product improvement could justify, for example, a mobile mapping application collecting precise, daily geolocation data about its customers and then retaining the data long after providing the service for which the data was necessary. Similarly, this commenter noted that companies potentially could use analytics programs to create very detailed consumer profiles to which many consumers might object, without offering them any choice. This commenter recommended that the Commission revise the proposed framework's internal operations category to make it consistent with the "operational purpose" language contained in H.R. 611 from the 112th Congress, which would include, among other things, "basic business functions such as accounting, inventory and supply chain management, quality assurance, and internal auditing."[182]

The Commission believes that for some practices, the benefits of providing choice are reduced – either because consent can be inferred or because public policy makes choice unnecessary. However, the Commission also appreciates the concerns that the preliminary staff report's definition of "commonly accepted practices" may have been both under-inclusive and over-inclusive. To the extent the proposed framework was interpreted to establish an inflexible list of specific practices, it risked undermining companies' incentives to innovate and develop new products and services to consumers, including innovative methods for reducing data collection while providing valued services. On the other hand, companies could read the definition so broadly that virtually any practice could be considered "commonly accepted."

The standard should be sufficiently flexible to allow for innovation and new business models but also should cabin the types of practices that do not require consumer choice. To strike that balance, the Commission refines the standard to focus on the *context of the interaction* between a business and the consumer. This new "context of the interaction" standard is similar to the concept suggested by some commenters that the need for choice should depend on reasonable consumer expectations,[183] but is intended to provide businesses with more concrete guidance. Rather than relying solely upon the inherently subjective test of consumer expectations, the revised standard focuses on more objective factors related to the consumer's relationship with a business. Specifically, whether a practice requires choice turns on the extent

181 *See Comment of Consumer Federation of America*, cmt. #00358, at 6.

182 *See Comment of Center for Democracy & Technology*, cmt. #00469, at 8-9 (citing BEST PRACTICES Act, H.R. 611, 112th Congress § 2(5)(iii) (2011).

183 *See Comment of Microsoft Corp.*, cmt. #00395, at 8; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 23-26; *Comment of Pharmaceutical Research & Manufacturers of America*, cmt. #00477, at 13.

to which the practice is consistent with the context of the transaction or the consumer's existing relationship with the business, or is required or specifically authorized by law.[184]

The purchase of an automobile from a dealership illustrates how this standard could apply. In connection with the sale of the car, the dealership collects personal information about the consumer and his purchase. Three months later, the dealership uses the consumer's address to send him a coupon for a free oil change. Similarly, two years after the purchase, the dealership might send the consumer notice of an upcoming sale on the type of tires that came with the car or information about the new models of the car. In this transaction the data collection and subsequent use is consistent with the context of the transaction and the consumer's relationship with the car dealership. Conversely, if the dealership sells the consumer's personal information to a third-party data broker that appends it to other data in a consumer profile to sell to marketers, the practice would not be consistent with the car purchase transaction or the consumer's relationship with the dealership.

Although the Commission has revised the standard for evaluating when choice is necessary, it continues to believe that the practices highlighted in the preliminary staff report – fulfilment, fraud prevention, internal operations, legal compliance and public purpose, and most first-party marketing[185] – provide illustrative guidance regarding the types of practices that would meet the revised standard and thus would not typically require consumer choice. Further, drawing upon the recommendations of several commenters,[186] the Commission agrees that the fraud prevention category would generally cover practices designed to prevent security attacks or phishing; internal operations would encompass frequency capping and similar advertising inventory metrics; and legal compliance and public purpose would cover intellectual property protection or using location data for emergency services.[187] It should be noted, however, that even within these categories there may be practices that are inconsistent with the context of the interaction standard and thus warrant consumer choice. For instance, there may be contexts in which the "repurposing" of data to improve existing products or services would exceed the internal operations concept. Thus, where a product improvement involves additional sharing of consumer data with third parties, it would no longer be an "internal operation" consistent with the context of the consumer's interaction with a company. On the

184 As noted above, focusing on the context of the interaction is consistent with the Respect for Context principle in the Consumer Privacy Bill of Rights proposed by the White House. *See* White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, App. A. (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. The Respect for Context principle requires companies to limit their use of consumer data to purposes that are consistent with the company's relationship with the consumer and with the context in which the consumer disclosed the data, unless the company is legally required to do otherwise. If a company will use data for other purposes it must provide a choice at a prominent point, outside of the privacy policy.

185 *See supra* at Section IV.C.1.

186 *See supra* note 175.

187 With respect to use of geolocation data for mapping, surveying or similar purposes, if the data cannot reasonably be linked to a specific consumer, computer, or device, a company collecting or using the data would not need to provide a consumer choice mechanism. Similarly, if a company takes reasonable measures to de-identify smart grid data and takes the other steps outlined above, the company would not be obligated to obtain consent before collecting or using the data. See *supra* Section IV.A.4.

other hand, product improvements such as a website redesign or a safety improvement would be the type of "internal operation" that is generally consistent with the context of the interaction.[188]

b. First-Party Marketing Generally Does Not Require Choice, But Certain Practices Raise Special Concerns.

The preliminary staff report's questions regarding first-party marketing generated a large number of comments. As discussed, the Commission has revised the standard for determining whether a practice requires consumer choice but believes that most first-party marketing practices are consistent with the consumer's relationship with the business and thus do not necessitate consumer choice. Nevertheless, as a number of the commenters discussed, there are certain practices that raise special concerns and therefore merit additional analysis and clarification.

(i) Companies Must Provide Consumers With A Choice Whether To Be Tracked Across Other Parties' Websites.

Commenters raised questions about companies and other services that have first-party relationships with consumers, but may have access to behavioral activity data that extends beyond the context of that first-party relationship. For example, in response to the question in the preliminary staff report regarding the use of deep packet inspection ("DPI"),[189] a number of commenters cited the ability of ISPs to use DPI to monitor and track consumers' movements across the Internet and use the data for marketing.[190] There appeared to be general consensus among the commenters that, based on the potential scope of the tracking, an ISP's use of DPI for marketing purposes is distinct from other forms of marketing practices by companies that have a first-party relationship with consumers, and thus at a minimum requires consumer choice.[191]

Similarly, commenters cited the use of "social plugins" – such as the Facebook "Like" button – that allow social media services to track consumers across every website that has installed the plugin.[192] The commenter stated that, as with DPI, consumers would not expect social media sites to track their visits to other websites or that the profiles created from such tracking could be used for marketing.

188 Moreover, even if a given practice does not necessitate consumer choice, the framework's other elements – *e.g.*, data collection limits and disposal requirements, increased transparency – would still apply, thereby preventing a company from exploiting these categories.

189 Deep packet inspection ("DPI") refers to the ability of ISPs to analyze the information, comprised of data packets, that traverses their networks when consumers use their services.

190 *See Comment of AT&T Inc.*, cmt. #00420, at 21-22 & n.34; *Comment of Berlin Commissioner for Data Protection & Freedom of Information*, cmt. #00484, at 2-3; *Comment of Computer & Communications Industry Ass'n*, cmt. #00434, at 15; *Comment of Phorm Inc.*, cmt. #00353, App. A at 3-4; *Comment of U.S. Public Policy Council of the Ass'n for Computing Machinery*, cmt. #00431, at 6.

191 *See Comment of Phorm Inc.*, cmt. #00353, App. A at 3-4; *Comment of Center for Democracy & Technology*, cmt. #00469, at 14-15; *Comment of AT&T Inc.*, cmt. #00420, at 21-22 & n.34.

192 *See Comment of Consumer Federation of America*, cmt. #00358, at 8 (citing Justin Brookman, *Facebook Pressed to Tackle Lingering Privacy Concerns*, Center for Democracy & Technology (June 16, 2010), *available at* https://www.cdt.org/blogs/justin-brookman/facebook-pressed-tackle-lingering-privacy-concerns); *Comment of Berkeley Center for Law & Technology*, cmt. #00347, at 8; *see also* Arnold Roosendaal, *Facebook Tracks and Traces Everyone: Like This!*, (Nov. 30, 2010), *available at* http://papers.ssrn.com/so13/papers.cfm?abstract_id=1717563 (detailing how Facebook tracks consumers through the Like button, including non-Facebook members and members who have logged out of their Facebook accounts); Nik Cubrilovic, *Logging Out Of Facebook Is Not Enough*, NEW WEB ORDER (Sept. 25, 2011), http://nikcub.appspot.com/posts/logging-out-of-facebook-is-not-enough.

The Commission agrees that where a company that has a first-party relationship with a consumer for delivery of a specific service but also tracks the consumer's activities across other parties' websites, such tracking is unlikely to be consistent with the context of the consumer's first-party relationship with the entity. Accordingly, under the final framework, such entities should not be exempt from having to provide consumers with choices. This is true whether the entity tracks consumers through the use of DPI, social plug-ins, http cookies, web beacons, or some other type of technology.[193]

As an example of how this standard can apply, consider a company with multiple lines of business, including a search engine and an ad network. A consumer has a "first-party relationship" with the company when using the search engine. While it may be consistent with this first-party relationship for the company to offer contextual ads on the search engine site, it would be inconsistent with the first-party search engine relationship for the company to use its third-party ad network to invisibly track the consumer across the Internet.

To use another example, many online retailers engage in the practice of "retargeting," in which the retailer delivers an ad to a consumer on a separate website based on the consumer's previous activity on the retailer's website.[194] Because the ad is tailored to the consumer's activity on the retailer's website, it could be argued that "retargeting" is a first-party marketing practice that does not merit consumer choice. However, because it involves tracking the consumer from the retailer's website to a separate site on which the retailer is a third party and communicating with the consumer in this new context, the Commission believes that the practice of retargeting is inconsistent with the context of consumer's first-party interaction with the retailer. Thus, where an entity has a first-party relationship with a consumer on its own website, and it engages in third-party tracking of the consumer across other websites the entity should provide meaningful choice to the consumer.

(ii) Affiliates Are Third Parties Unless The Affiliate Relationship Is Clear to Consumers.

Several trade organizations stated that first-party marketing should include the practice of data sharing among all of a particular entity's corporate affiliates and subsidiaries.[195] In contrast, a number of commenters – including individual companies and consumer advocates – took a more limited approach that would treat affiliate sharing as a first-party practice only if the affiliated companies share a trademark, are commonly-branded, or the affiliated relationship is otherwise reasonably clear to consumers.[196] One consumer advocate also suggested restricting data sharing to commonly-branded affiliates in the same line of business so that the data would be used in a manner that is consistent with the purpose for which the first party collected it.[197]

193 See *infra* at Section IV.C.2.d. (discussing special concerns that arise by comprehensive tracking by large platform providers).

194 For example, a consumer visits an online sporting goods retailer, looks at but does not purchase running shoes, and then visits a different website to read about the local weather forecast. A first party engages in retargeting if it delivers an ad for running shoes to the consumer on the third-party weather site.

195 *See Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 16; *Comment of Interactive Advertising Bureau*, cmt. #00388, at 8; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 24.

196 *See Comment of Yahoo! Inc.*, cmt. #00444, at 11; *Comment of IBM*, cmt. #00433, at 6; *Comment of AT&T Inc.*, cmt. #00420, at 20; *Comment of Catalog Choice*, cmt. #00473, at 10; *Comment of Consumers Union*, cmt. #00362, at 10-11.

197 *See Comment of Consumers Union*, cmt. #00362, at 10-11.

The Commission maintains the view that affiliates are third parties, and a consumer choice mechanism is necessary unless the affiliate relationship is clear to consumers. Common branding is one way of making the affiliate relationship clear to consumers. By contrast, where an affiliate relationship is hidden – such as between an online publisher that provides content to consumers through its website and an ad network that invisibly tracks consumers' activities on the site – marketing from the affiliate would not be consistent with a transaction on, or the consumer's relationship with, that website. In this scenario consumers should receive a choice about whether to allow the ad network to collect data about their activities on the publisher's site.

(iii) Cross-Channel Marketing Is Generally Consistent with the Context of a Consumer's Interaction with a Company.

A variety of commenters also discussed the issue of whether the framework should require choice for cross-channel marketing, *e.g.*, where a consumer makes an in-store purchase and receives a coupon – not at the register, but in the mail or through a text message. These commenters stated that the framework should not require choice when a first party markets to consumers through different channels, such as the Internet, email, mobile apps, texts, or in the offline context.[198] In support of this conclusion, one commenter stated that restricting communications from a first party to the initial means of contact would impose costs on business without any consumer benefits.[199]

The Commission agrees that the first-party marketing concept should include the practice of contacting consumers across different channels. Regardless of the particular means of contact, receipt of a message from a company with which a consumer has interacted directly is likely to be consistent with the consumer's relationship with that company.[200] At the same time, as noted above, if an offline or online retailer tracks a customer's activities on a third-party website, this is unlikely to be consistent with the customer's relationship with the retailer; thus, choice should be required.

(iv) Companies Should Implement Measures to Improve The Transparency of Data Enhancement.

A large number of commenters discussed whether the practice of data enhancement, by which a company appends data obtained from third-party sources to information it collects directly from consumers, should require choice. Some of these commenters specifically objected to allowing companies to enhance data without providing consumers choice about the practice.[201]

For example, one academic organization characterized data enhancement without consumer choice as "trick[ing]" consumers into participating in their own profiling for the benefit of companies.[202] As

198 *See Comment of Yahoo! Inc.*, cmt. #00444, at 10; *Comment of IBM*, cmt. #00433, at 6; *Comment of AT&T Inc.*, cmt. #00420, at 20; *Comment of Catalog Choice*, cmt. #00473, at 9-10; *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 16; *Comment of Interactive Advertising Bureau*, cmt. #00388, at 8.

199 *See Comment of American Catalog Mailers Ass'n*, cmt. #00424, at 7.

200 Such marketing communications would, of course, still be subject to any existing restrictions, including the CAN-SPAM Act, 15 U.S.C. §§ 7701-7713 (2010).

201 *See Comment of Consumer Federation of America*, cmt. #00358, at 10; *Comment of Consumers Union*, cmt. #00362, at 11.

202 *Comment of Berkeley Center for Law & Technology*, cmt. #00347, at 9-10.

companies develop new means for collecting data about individuals, this commenter stated, consumers should have more tools to control data collection, not fewer.[203]

Similarly, a consumer organization explained that consumers may not anticipate that the companies with which they have a relationship can obtain additional data about them from other sources, such as social networking sites, and use the data for marketing.[204] This commenter concluded that requiring companies to provide choice will necessitate better explanations of the practice, which will lead to improved consumer understanding.

Other stakeholders also raised concerns about data enhancement absent consumer choice. One company focused on the practice of enhancing online cookie data or IP addresses with offline identity data and stated that such enhancement should be subject to consumer choice.[205] In addition, a data protection authority stated that consumers are likely to expect choice where the outcome of data enhancement could negatively affect the consumer or where the sources of data used for enhancement would be unexpected to the consumer.[206]

Alternatively, a number of industry commenters opposed requiring consumer choice for data enhancement in connection with first-party marketing. These commenters described data enhancement as a routine and longstanding practice that allows businesses to better understand and serve their consumers.[207] Commenters enumerated a variety of benefits from the availability and use of third-party data, including: development of new or more relevant products and services; ensuring the accuracy of databases; reducing barriers to small firms seeking to enter markets; helping marketers identify the best places to locate retail stores; and reducing irrelevant marketing communications.[208]

One commenter noted that requiring content publishers such as newspapers to offer consumer choice before buying information from non-consumer-facing data brokers would impose logistical and financial challenges that would interfere with publishers' ability to provide relevant content or sell the advertising to support it.[209] Other commenters claimed that, where the data used for enhancement comes from third-party sources, it was likely subject to choice at the point of collection from the consumer and therefore providing additional choice is unnecessary.[210] Taking a similar approach, one company noted that the third-party source of the data should be responsible for complying with the framework when it shares data, and the recipient should be responsible for any subsequent sharing of the enhanced data.[211]

203 *Id.*, at 8-10 (describing Williams-Sonoma's collection of consumers' zip codes in *Pineda v. Williams-Sonoma Stores, Inc.*, 246 P.3d 612 (Cal. 2011)).

204 *Comment of Consumer Federation of America*, cmt. #00358, at 10.

205 *See Comment of Phorm Inc.*, cmt. #00353, at 5.

206 *See Comment of the Information Commissioner's Office of the UK*, cmt. #00249, at 3.

207 *See Comment of Newspaper Ass'n of America*, cmt. #00383, at 7-8; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 24-26; *Comment of Experian*, cmt. #00398, at 5-6; *Comment of Magazine Publishers of America*, cmt. #00332, at 4; *Consumer Data Industry Ass'n*, cmt. #00363, at 2-3.

208 *Comment of Experian*, cmt. #00398, at 6; *see Comment of Newspaper Ass'n of America*, cmt. #00383, at 6-8.

209 *Comment of Newspaper Ass'n of America*, cmt. #00383, at 7-8.

210 *Comment of Experian*, cmt. #00398, at 9 (citing the Direct Marketing Association's Guidelines for Ethical Business Practice); *Comment of Magazine Publishers of America*, cmt. #00332, at 5-6.

211 *Comment of Microsoft Corp.*, cmt. #00395, at 8.

The issue of whether a first-party marketer should provide choice for data enhancement is particularly challenging because the practice involves two separate and distinct types of consumer data collection. One involves the consumer-to-business transfer of data – for instance, where an online retailer collects information directly from the consumer by tracking the products the consumer purchased in the store or looked at while visiting the retailer's website. The other involves a business-to-business transfer of data – such as where retailer purchases consumer data from a non-consumer-facing data broker.

As to the first type of data collection, for the reasons discussed above, if the first party does not share information with third parties or track consumers across third-party websites, the practice would be consistent with the context of the consumer's interaction with the company.[212] Therefore, the framework would not call for a consumer choice mechanism. In contrast, because the second type of data collection involves the transfer of data from one business to another and does not directly involve the consumer (and therefore is typically unknown to the consumer), it is unlikely to be consistent with a transaction or relationship between the consumer and the first party. The Commission nevertheless recognizes that it would be impractical to require the first-party marketer to offer a choice mechanism when it appends data from third-party sources to the data it collects directly from its consumers. As discussed in the comments, such a requirement would impose costs and logistical problems that could preclude the range of benefits that data enhancement facilitates.

Instead, full implementation of the framework's other components should address the privacy concerns that commenters raised about data enhancement. First, companies should incorporate privacy by design concepts, including limiting the amount of data they collect from consumers and third parties alike to accomplish a specific business purpose, reducing the amount of time they retain such data, and adopting reasonable security measures. The framework also calls for consumer choice where a company shares with a third party the data it collects from a consumer. Thus, consumers will have the ability to control the flow of their data to third parties who might sell the data to others for enhancement. In addition, companies should improve the transparency of their practices by disclosing that they engage in data enhancement and educating consumers about the practice, identifying the third-party sources of the data, and providing a link or other contact information so the consumer can contact the third-party source directly. Finally, to further protect consumer privacy, the Commission recommends that first parties that obtain marketing data for enhancement should take steps to encourage their third-party data broker sources to increase their own transparency, including by participating in a centralized data broker website, discussed further below, where consumers could learn more information about data brokers and exercise choices.[213] The first parties may also consider contractually requiring their data broker sources to take these steps.

Not much discussion on linking...

212 See *supra* Section IV.C.1.b.(i).

213 The concept of such a website is discussed, *infra*, Section IV.D.2.a.

DATA ENHANCEMENT CASE STUDY: FACIAL RECOGNITION SOFTWARE

Facial recognition technology[1] enables the identification of an individual based on his or her distinct facial characteristics. While this technology has been used in experiments for over thirty years, until recently it remained costly and limited under real world conditions.[2] However, steady improvements in the technology combined with increased computing power have shifted this technology out of the realm of science fiction and into the marketplace. As costs have decreased and accuracy improved, facial recognition software has been incorporated into a variety of commercial products. Today it can be found in online social networks and photo management software, where it is used to facilitate photo-organizing,[3] and in mobile apps where it is used to enhance gaming.[4]

This surge in the deployment of facial recognition technology will likely boost the desire of companies to use data enhancement by offering yet another means to compile and link information about an individual gathered through disparate transactions and contexts. For instance, social networks such as Facebook and LinkedIn, as well as websites like Yelp and Amazon, all encourage users to upload profile photos and make these photos publicly available. As a result, vast amounts of facial data, often linked with real names and geographic locations, have been made publicly available. A recent paper from researchers at Carnegie Mellon University illustrated how they were able to combine readily available facial recognition software with data mining algorithms and statistical re-identification techniques to determine in many cases an individual's name, location, interests, and even the first five digits of the individual's Social Security number, starting with only the individual's picture.[5]

Companies could easily replicate these results. Today, retailers use facial *detection* software in digital signs to analyze the age and gender of viewers and deliver targeted advertisements.[6] Facial detection does not uniquely identify an individual. Instead, it detects human faces and determines gender and approximate age range. In the future, digital signs and kiosks placed in supermarkets, transit stations, and college campuses could capture images of viewers and, through the use of facial *recognition* software, match those faces to online identities, and return advertisements based on the websites specific individuals have visited or the publicly available information contained in their social media profiles. Retailers could also implement loyalty programs, ask users to associate a photo with the account, then use the combined data to link the consumer to other online accounts or their in-store actions. This would enable the retailer to glean information about the consumer's purchase habits, interests, and even movements,[7] which could be used to offer discounts on particular products or otherwise market to the consumer.

The ability of facial recognition technology to identify consumers based solely on a photograph, create linkages between the offline and online world, and compile highly detailed dossiers of information, makes it especially important for companies using this technology to implement privacy by design concepts and robust choice and transparency policies. Such practices should include reducing the amount of time consumer information is retained, adopting reasonable security measures, and disclosing to consumers that the facial data they supply may be used to link them to information from third parties or publicly available sources. For example, if a digital sign uses data enhancement to deliver targeted advertisements to viewers, it should immediately delete the data after the consumer has walked away. Likewise, if a kiosk is used to invite shoppers to register for a store loyalty program, the shopper should be informed that the photo taken by the kiosk camera and associated with the account may be combined with other data to market discounts and offers to the shopper. If a company received the data from other sources, it should disclose the sources to the consumer.

NOTES

1 The Commission held a facial recognition workshop on December 8, 2011. *See* FTC Workshop, *Face Facts: A Forum on Facial Recognition Technology* (Dec. 8, 2011), http://www.ftc.gov/bcp/workshops/facefacts/.

2 *See* Alessandro Acquisti *et al.*, *Faces of Facebook: Privacy in the Age of Augmented Reality*, http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/.

3 *See* Justin Mitchell, *Making Photo Tagging Easier*, The Facebook Blog (June 30, 2011, 5:16 PM), https://blog.facebook.com/blog.php?post=467145887130; Matt Hickey, *Picasa Refresh Brings Facial Recognition*, TechCrunch (Sept. 2, 2008), http://techcrunch.com/2008/09/02/picasa-refresh-brings-facial-recognition/.

4 *See* Tomio Geron, *Viewdle Launches 'Third Eye' Augmented Reality Game*, Forbes, June 22, 2011, *available at* http://www.forbes.com/sites/tomiogeron/2011/06/22/viewdle-lauches-third-eye-augmented-reality-game/.

5 *See* Alessandro Acquisti *et al.*, *Faces of Facebook: Privacy in the Age of Augmented Reality*, http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/.

6 *See* Shan Li & David Sarno, *Advertisers Start Using Facial Recognition to Tailor Pitches*, L.A. Times, Aug. 21, 2011, *available at* http://articles.latimes.com/2011/aug/21/business/la-fi-facial-recognition-20110821.

7 For instance, many consumers use services such as Foursquare which allow them to use their mobile phone to "check in" at a restaurant to find friends who are nearby. *See* Foursquare, About Foursquare, https://foursquare.com/about.

(v) Companies Should Generally Give Consumers a Choice Before Collecting Sensitive Data for First-Party Marketing.

Commenters addressed whether companies that collect sensitive data[214] for their own marketing should offer consumer choice. A number of privacy and consumer organizations asserted that even where a business collects data in a first-party setting, any marketing based on sensitive data should require the consumer's affirmative express consent.[215] These commenters stated that the use of sensitive data for marketing could cause embarrassment for consumers or lead to various types of discriminatory conduct, including denial of benefits or being charged higher prices. One such commenter also noted that heightened choice for sensitive data is consistent with the FTC staff's Self-Regulatory Principles for Online Behavioral Advertising ("2009 OBA Report").[216]

Rather than always requiring consent, an industry trade association pushed for a more flexible approach to the use of sensitive data in first-party marketing.[217] This commenter stated that the choice analysis should depend upon the particular context and circumstances in which the data is used. The commenter noted that, for example, with respect to sensitive location data, where a consumer uses a wireless service to find nearby restaurants and receive discounts, the consumer implicitly understands his location data will be used and consent can be inferred.

The Commission agrees with the commenters who stated that affirmative express consent is appropriate when a company uses sensitive data for any marketing, whether first- or third-party. Although, as a general rule, most first-party marketing presents fewer privacy concerns, the calculus changes when the data is sensitive. Indeed, when health or children's information is involved, for example, the likelihood that data misuse could lead to embarrassment, discrimination, or other harms is increased. This risk exists regardless of whether the entity collecting and using the data is a first party or a third party that is unknown to the consumer. In light of the heightened privacy risks associated with sensitive data, first parties should provide a consumer choice mechanism at the time of data collection.[218]

At the same time, the Commission believes this requirement of affirmative express consent for first-party marketing using sensitive data should be limited. Certainly, where a company's business model is *designed to target* consumers based on sensitive data – including data about children, financial and health information, Social Security numbers, and certain geolocation data – the company should seek affirmative express consent before collecting the data from those consumers.[219] On the other hand, the risks to consumers may not justify the potential burdens on general audience businesses that *incidentally collect* and use sensitive

214 The Commission defines as sensitive, at a minimum, data about children, financial and health information, Social Security numbers, and certain geolocation data, as discussed below. See *infra* Section IV.C.2.e.(ii).

215 *Comment of Center for Democracy & Technology*, cmt. #00469, at 10; *Comment of Consumer Federation of America*, cmt. #00358, at 8-9; *Comment of Consumers Union*, cmt. #00362, at 12-13.

216 *See Comment of Center for Democracy & Technology*, cmt. #00469 at 10 (citing FTC, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, 43-44 (2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf).

217 *Comment of CTIA – The Wireless Ass'n*, cmt. #00375, at 4-6.

218 Additional discussion regarding the necessary level of consent for the collection or use of sensitive data, as well as other practices that raise special privacy considerations, is set forth below. See *infra* Section IV.C.2.e.(ii).

219 These categories of sensitive data are discussed further below. See *infra* Section IV.C.2.e.(ii).

information. For example, the Commission has previously noted that online retailers and services such as Amazon.com and Netflix need not provide choice when making product recommendations based on prior purchases. Thus, if Amazon.com were to recommend a book related to health or financial issues based on a prior purchase on the site, it need not provide choice. However, if a health website is designed to target people with particular medical conditions, that site should seek affirmative express consent when marketing to consumers.

Final Principle: Companies do not need to provide choice before collecting and using consumer data for practices that are consistent with the context of the transaction or the company's relationship with the consumer, or are required or specifically authorized by law.

2. FOR PRACTICES INCONSISTENT WITH THE CONTEXT OF THEIR INTERACTION WITH CONSUMERS, COMPANIES SHOULD GIVE CONSUMERS CHOICES.

Proposed Principle: For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data.

For those practices for which choice is contemplated, the proposed framework called on companies to provide choice at a time and in a context in which the consumer is making a decision about his or her data. In response, commenters discussed a number of issues, including the methods for providing just in time choice, when "take-it-or-leave-it" choice may be appropriate, how to respond to the call for a Do Not Track mechanism that would allow consumers to control online tracking, and the contexts in which affirmative express consent is necessary.

The Commission adopts the proposed framework's formulation that choice should be provided at a time and in a context in which the consumer is making a decision about his or her data. The Commission also adds new language addressing when a company should seek a consumer's affirmative express consent.

a. Companies Should Provide Choices At a Time and In a Context in Which the Consumer Is Making a Decision About His or Her Data.

The call for companies to provide a "just in time" choice generated numerous comments. Several consumer organizations as well as industry commenters stressed the importance of offering consumer choice at the time the consumer provides – and the company collects or uses – the data at issue and pointed to examples of existing mechanisms for providing effective choice.[220] One commenter stated that in order to make choice mechanisms meaningful to consumers, companies should incorporate them as a feature of a product or service rather than as a legal disclosure.[221] Using its vendor recommendation service as an example, this commenter suggested incorporating a user's sharing preferences into the sign-up process instead of setting such preferences as a default that users can later adjust and personalize. Another

220 *See Comment of Consumer Federation of America*, cmt. #00358, at 10; *Comment of Center for Democracy & Technology*, cmt. #00469, at 23-24; *Comment of AT&T Inc.*, cmt. #00420, at 22-23; *Comment of Phorm Inc.*, cmt. #00353, at 9-10.

221 *Comment of AT&T Inc.*, cmt. #00420, at 22-23.

commenter stated that choice options should occur in a "time-appropriate manner" that takes into account the "functional and aesthetic context" of the product or service.[222]

Others raised concerns about the practicality of providing choice prior to the collection or use of data in different contexts.[223] For instance, a number of commenters discussed the offline retail context and noted that cashiers are typically unqualified to communicate privacy information or to discuss data collection and use practices with customers.[224] One commenter further discussed the logistical problems with providing such information at the point of sale, citing consumer concerns about ease of transaction and in-store wait times.[225] Other commenters described the impracticality of offering and obtaining advance consent in an offline mail context, such as a magazine subscription card or catalogue request that a consumer mails to a fulfillment center.[226] In the online context, one commenter expressed concern that "pop-up" choice mechanisms complicate or clutter the user experience, which could lead to choice "fatigue."[227] Another commenter noted that where data collection occurs automatically, such as in the case of online behavioral advertising, obtaining consent before collection could be impractical.[228]

One theme that a majority of the commenters addressing this issue articulated is the need for flexibility so that companies can tailor the choice options to specific business models and contexts.[229] Rather than a rigid reliance on advance consent, commenters stated that companies should be able to provide choice before collection, close to the time of collection, or a time that is convenient to the consumer.[230] The precise method should depend upon context, the sensitivity of the data at issue, and other factors.[231] Citing its own best practices guidance, one trade organization recommended that the Commission focus not on the precise mechanism for offering choice, but on whether the consent is informed and based on sufficient notice.[232]

The Commission appreciates the concerns that commenters raised about the timing of providing choices. Indeed, the proposed framework was not intended to set forth a "one size fits all" model for designing consumer choice mechanisms. Staff instead called on companies to offer clear and concise choice

222 *Comment of Center for Democracy & Technology*, cmt. #00469, at 11.

223 *See Comment of Microsoft Corp.*, cmt. #00395, at 8-10, 14; *Comment of SIFMA*, cmt. #00265, at 5-6; *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 8-10.

224 *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 8; *Comment of Experian*, cmt. #00398, at 9.

225 *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 8.

226 *See Comment of Magazine Publishers of America*, cmt. #00332, at 4 (noting that the "blow-in cards" in magazines often used to solicit new subscriptions have very limited space, and including lengthy disclosures on these cards could render them unreadable); *Comment of American Catalogue Mailers Ass'n*, cmt. #00424, at 7.

227 *See Comment of Retail Industry Leaders Ass'n*, cmt. #00352 at 7; *see also Comment of Experian*, cmt. #00398, at 9 (noting that the proposed changes in notice and choice procedures would be inconvenient for consumers and would damage the consumer experience).

228 *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 8.

229 *Comment of Microsoft Corp.*, cmt. #00395, at 2; *Comment of AT&T Inc.*, cmt. #00420 at 3, 7; *Comment of Consumers Union*, cmt. #00362, at 5, 11-12; *Comment of Consumer Federation of America*, cmt. #00358, at 10.

230 *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 9.

231 *Comment of Facebook, Inc.*, cmt. #00413, at 10; *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 9; *see also Comment of Experian*, cmt. #00398, at 9 (generally disputing the need for "just-in-time" notice, but acknowledging that it might be justified for the transfer to non-affiliated third parties of sensitive information for marketing purposes).

232 *See Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 10 (describing the form of consent outlined in the CTIA's "Best Practices and Guidelines for Location-Based Services").

mechanisms that are easy to use and are delivered at a time and in a context that is relevant to the consumer's decision about whether to allow the data collection or use. Precisely how companies in different industries achieve these goals may differ depending on such considerations as the nature or context of the consumer's interaction with a company or the type or sensitivity of the data at issue.

In most cases, providing choice before or at the time of collection will be necessary to gain consumers' attention and ensure that the choice presented is meaningful and relevant. If a consumer is submitting his or her data online, the consumer choice could be offered, for example, directly adjacent to where the consumer is entering his or her data. In other contexts, the choice might be offered immediately upon signing up for a service, as in the case of a social networking website.

In some contexts, however, it may be more practical to communicate choices at a later point. For example, in the case of an offline retailer, the choice might be offered close to the time of a sale, but in a manner that will not unduly interfere with the transaction. This could include communicating the choice mechanism through a sales receipt or on a prominent poster at the location where the transaction takes place. In such a case, there is likely to be a delay between when the data collection takes place and when the consumer is able to contact the company in order to exercise any choice options. Accordingly, the company should wait for a disclosed period of time before engaging in the practices for which choice is being offered.[233] The Commission also encourages companies to examine the effectiveness of such choice mechanisms periodically to determine whether they are sufficiently prominent, effective, and easy to use.

Industry is well positioned to design and develop choice mechanisms that are practical for particular business models or contexts, and that also advance the fundamental goal of giving consumers the ability to make informed and meaningful decisions about their privacy. The Commission calls on industry to use the same type of creativity industry relies on to develop effective marketing campaigns and user interfaces for consumer choice mechanisms. One example of such a creative approach is the online behavioral advertising industry's development of a standardized icon and text that is embedded in targeted advertisements. The icon and text are intended to communicate that the advertising may rely on data collected about consumers. They also serve as a choice mechanism to allow the consumer to exercise control over the delivery of such ads.[234] Even though in most cases, cookie placement has already occurred, the in-ad disclosure provides a logical "teachable moment" for the consumer who is making a decision about his or her data.[235]

b. Take-it-or-Leave-it Choice for Important Products or Services Raises Concerns When Consumers Have Few Alternatives.

Several commenters addressed whether it is appropriate for a company to make a consumer's use of its product or service contingent upon the consumer's acceptance of the company's data practices. Two industry

233 The FTC recognizes that incorporating this delay period may require companies to make programming changes to their systems. As noted above, in the discussion of legacy data systems, see *supra* at Section IV.B.2., these changes may take time to implement.

234 As noted in Section IV.C.2.c., industry continues to consider ways to make the icon and opt out mechanism more usable and visible for consumers.

235 *But see Comment of Center for Digital Democracy and U.S. PIRG*, cmt. #00338, at 29 (criticizing visibility of the icon to consumers).

for example, the purchase of an important product that has few substitutes, such as a patented medical device. If a company offered a limited warranty for the device only in exchange for the consumer's agreeing to disclose his or her income, religion, and other highly-personal information, the consumer would not have been offered a meaningful choice and a take-it-or-leave approach would be inappropriate.

Another example is the provision of broadband Internet access. As consumers shift more aspects of their daily lives to the Internet – shopping, interacting through social media, accessing news, entertainment, and information, and obtaining government services – broadband has become a critical service for many American consumers. When consumers have few options for broadband service, the take-it-or-leave-it approach becomes one-sided in favor of the service provider. In these situations, the service provider should not condition the provision of broadband on the customer's agreeing to, for example, allow the service provider to track all of the customer's online activity for marketing purposes. Consumers' privacy interests ought not to be put at risk in such one-sided transactions.

With respect to less important products and services in markets with sufficient alternatives, take-it-or-leave-it choice can be acceptable, provided that the terms of the exchange are transparent and fairly disclosed – *e.g.*, "we provide you with free content in exchange for collecting information about the websites you visit and using it to market products to you." Under the proper circumstances, such choice options may result in lower prices or other consumer benefits, as companies develop new and competing ways of monetizing their business models.

c. Businesses Should Provide a Do Not Track Mechanism To Give Consumers Control Over the Collection of Their Web Surfing Data.

Like the preliminary staff report, this report advocates the continued implementation of a universal, one-stop choice mechanism for online behavioral tracking, often referred to as Do Not Track. Such a mechanism should give consumers the ability to control the tracking of their online activities.

Many commenters discussed the progress made by industry in developing such a choice mechanism in response to the recommendations of the preliminary staff report and the 2009 OBA Report, and expressed support for these self-regulatory initiatives.[246] These initiatives include the work of the online advertising industry over the last two years to simplify disclosures and improve consumer choice mechanisms; efforts by the major browsers to offer new choice mechanisms; and a project of a technical standards body to

246 *See, e.g.*, *Comment of American Ass'n of Advertising Agencies et. al*, cmt. #00410, at 3 (describing the universal choice mechanisms used in the coalition's Self-Regulatory Principles for Online Behavioral Advertising Program); *Comment of BlueKai*, cmt. #00397, at 3 (describing its development of the NAI Opt-Out Protector for Firefox); *Comment of Computer & Communications Industry Ass'n*, cmt. #00434, at 17 (describing both company-specific and industry-wide opt-out mechanisms currently in use); *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 3 (stating that the Self-Regulatory Principles for Online Behavioral Advertising Program addresses the concerns that motivate calls for a "Do-Not-Track" mechanism); *Comment of Facebook, Inc.*, cmt. #00413, at 13 (describing behavioral advertising opt-out mechanisms developed by both browser makers and the advertising industry); *Comment of Future of Privacy Forum*, cmt. #00341, at 2-4 (describing the development of a browser-based Do-Not-Track header and arguing that the combined efforts of browser companies, ad networks, consumers, and government are likely to result in superior choice mechanisms); *Comment of Google, Inc.*, cmt. #00417, at 5 (describing its Ad Preferences Manager and Keep My Opt-Outs tools); *Comment of Interactive Advertising Bureau*, cmt. #00388, at 5-7 (describing the Self-Regulatory Principles for Online Behavioral Advertising Program); *Comment of Microsoft Corp.*, cmt. #00395, at 11-14 (describing a variety of browser-based and ad network-based choice tools currently available); *Comment of U.S. Chamber of Commerce*, cmt. #00452, at 5-6 (describing a variety of browser-based and ad network-based choice tools currently available).

commenters suggested that "take-it-or-leave-it" or "walk away" choice is common in many business models, such as retail and software licensing, and companies have a right to limit their business to those who are willing to accept their policies.[236] Another commenter stated that preventing companies from offering take-it-or-leave-it choice might be unconstitutional under the First Amendment.[237] Other commenters, however, characterized walk away choice as generally inappropriate.[238] Some argued that the privacy framework should prevent companies from denying consumers access to goods or services, including website content, where consumers choose to limit the collection or use of their data.[239]

Most of the commenters that addressed this issue took a position somewhere in between.[240] In determining whether take-it-or-leave-it choice is appropriate, these commenters focused on three main factors. First, they noted that there must be adequate competition, so that the consumer has alternative sources to obtain the product or service in question.[241] Second, they stated that the transaction must not involve an essential product or service.[242] Third, commenters stated that the company offering take-it-or-leave-it choice must clearly and conspicuously disclose the terms of the transaction so that the consumer is able to understand the value exchange. For example, a company could clearly state that in exchange for receiving a service at "no cost," it collects certain information about your activity and sells it to third parties.[243] Expanding upon this point, commenters stressed that to ensure consumer understanding of the nature of the take-it-or-leave-it bargain, the disclosure must be prominent and not buried within a privacy policy.[244]

The Commission agrees that a "take it or leave it" approach is problematic from a privacy perspective, in markets for important services where consumers have few options.[245] For such products or services, businesses should not offer consumers a "take it or leave it" choice when collecting consumers' information in a manner inconsistent with the context of the interaction between the business and the consumer. Take,

236 *Comment of Performance Marketing Ass'n*, cmt. #00414, at 6; *Comment of Business Software Alliance,* cmt. #00389, at 11-12.

237 *Comment of Tech Freedom*, cmt. #00451, at 17.

238 *Comment of Consumer Federation of America*, cmt. #00358, at 11; *Comment of ePrio, Inc.*, cmt. #00267, at 4-5.

239 *Comment of Consumer Federation of America*, cmt. #00358, at 11; *see also Comment of Consumers Union,* cmt. #00362, at 12 (urging that consumers who choose to restrict sharing of their PII with unknown third parties should not be punished for that choice).

240 *See, e.g., Comment of Center for Democracy & Technology*, cmt. #00469, at 13 (stating that it has no objection to take-it-or-leave-it approaches, provided there is competition and the transaction does not involve essential services); *Comment of Microsoft Corp.*, cmt. #00395, at 10 (stating that take-it-or-leave-it choice is appropriate provided the "deal" is made clear to the consumer); *Comment of the Information Commissioner's Office of the UK,* cmt. #00249, at 4 (stating that take-it-or-leave-it choice would be inappropriate where the consumer has no real alternative but to use the service); *Comment of Reed Elsevier, Inc.*, cmt. #00430, at 11 (stating that while acceptable for the websites of private industry, websites that provide a public service and may be the single source of certain information, such as outsourced government agency websites, should not condition their use on take-it-or-leave-it terms).

241 *Comment of Center for Democracy & Technology*, cmt. #00469, at 13; *Comment of the Information Commissioner's Office of the UK,* cmt. #00249, at 4.

242 *Comment of Center for Democracy & Technology,* cmt. #00469, at 13; *Comment of Reed Elsevier, Inc.*, cmt. #00430, at 11.

243 *Comment of Microsoft Corp.*, cmt. #00395, at 10; *see also Comment of Center for Democracy & Technology,* cmt. #00469, at 13 (stating that the terms of the bargain should be clearly and conspicuously disclosed).

244 *Comment of TRUSTe*, cmt. #00450, at 11; *see also Comment of Center for Democracy & Technology*, cmt. #00469, at 13 (stating that terms should be "transparent and fairly presented").

245 This Report is not intended to reflect Commission guidance regarding Section 5's prohibition on unfair methods of competition.

standardize opt outs for online tracking.[247] A number of commenters, however, expressed concerns that existing mechanisms are still insufficient. Commenters raised questions about the effectiveness and comprehensiveness of existing mechanisms for exercising choice and the legal enforceability of such mechanisms.[248] Due to these concerns, some commenters advocated for legislation mandating a Do Not Track mechanism.[249]

The Commission commends recent industry efforts to improve consumer control over behavioral tracking and looks forward to final implementation. As industry explores technical options and implements self-regulatory programs, and Congress examines Do Not Track, the Commission continues to believe that in order to be effective, any Do Not Track system should include five key principles. First, a Do Not Track system should be implemented universally to cover all parties that would track consumers. Second, the choice mechanism should be easy to find, easy to understand, and easy to use. Third, any choices offered should be persistent and should not be overridden if, for example, consumers clear their cookies or update their browsers. Fourth, a Do Not Track system should be comprehensive, effective, and enforceable. It should opt consumers out of behavioral tracking through any means and not permit technical loopholes.[250] Finally, an effective Do Not Track system should go beyond simply opting consumers out of receiving targeted advertisements; it should opt them out of collection of behavioral data for all purposes other than those that would be consistent with the context of the interaction (*e.g.*, preventing click-fraud or collecting de-identified data for analytics purposes).[251]

Early on the companies that make web browsers stepped up to the challenge to give consumers choice about how they are tracked online, sometimes known as the "browser header" approach. The browser header is transmitted to all types of entities, including advertisers, analytics companies, and researchers, that track consumers online. Just after the FTC's call for Do Not Track, Microsoft developed a system to let users of Internet Explorer prevent tracking by different companies and sites.[252] Mozilla introduced a Do Not Track privacy control for its Firefox browser that an impressive number of consumers have adopted.[253]

---

247 *See supra* at Section II.C.1.

248 *Comment of American Civil Liberties Union*, cmt. #00425, at 12; *Comment of Center for Digital Democracy and U.S. PIRG*, cmt. #00338, at 28; *Comment of Consumer Federation of America*, cmt. #00358, at 13; *Comment of Consumers Union*, cmt. #00362, at 14; *see also Comment of World Privacy Forum*, cmt. #00369, at 3 (noting prior failures of self-regulation in the online advertising industry).

249 *E.g., Comment of Consumers Union*, cmt. #00362, at 14; *Comment of World Privacy Forum*, cmt. #00369, at 3.

250 For example, consumers may believe they have opted out of tracking if they block third-party cookies on their browsers; yet they may still be tracked through Flash cookies or other mechanisms. The FTC recently brought an action against a company that told consumers they could opt out of tracking by exercising choices through their browsers; however, the company used Flash cookies for such tracking, which consumers could not opt out of through their browsers. *In the Matter of ScanScout, Inc.*, FTC Docket No. C-4344 (Dec. 21, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023185/111221scanscoutdo.pdf.

251 Such a mechanism should be different from the Do Not Call program in that it should not require the creation of a "Registry" of unique identifiers, which could itself cause privacy concerns.

252 *Comment of Microsoft Corp.*, cmt. #00395, at 12.

253 *Comment of Mozilla*, cmt. #00480, at 2; Alex Fowler, *Do Not Track Adoption in Firefox Mobile is 3x Higher than Desktop*, Mozilla Privacy Blog, (Nov. 2, 2011), http://blog.mozilla.com/privacy/2011/11/02/do-not-track-adoption-in-firefox-mobile-is-3x-higher-than-desktop/.

Apple subsequently included a similar Do Not Track control in Safari.[254] Google has taken a slightly different approach – providing consumers with a tool that persistently opts them out of most behavioral advertising.[255]

In another important effort, the online advertising industry, led by the DAA, has implemented a behavioral advertising opt-out program. The DAA's accomplishments are notable: it has developed a notice and choice mechanism through a standard icon in ads and on publisher sites; deployed the icon broadly, with over 900 billion impressions served each month; obtained commitments to follow the self-regulatory principles from advertisers, ad networks, and publishers that represent close to 90 percent of the online behavioral advertising market; and established an enforcement mechanism designed to ensure compliance with the principles.[256] More recently, the DAA addressed one of the long-standing criticisms of its approach – how to limit secondary use of collected data so that the consumer opt out extends beyond simply blocking targeted ads to the collection of information for other purposes. The DAA has released new principles that include limitations on the collection of tracking data and prohibitions on the use or transfer of the data for employment, credit, insurance, or health care eligibility purposes.[257] Just as important, the DAA recently moved to address some persistence and usability criticisms of its icon-based opt out by committing to honor the tracking choices consumers make through their browser settings.[258]

At the same time, the W3C Internet standards-setting body has gathered a broad range of stakeholders to create an international, industry-wide standard for Do Not Track. The group includes a wide variety of stakeholders, including DAA members; other U.S. companies; international companies; industry groups; and public-interest groups. The W3C group has done admirable work to flesh out the details required to make a Do Not Track system practical in both desktop and mobile settings. The group has issued two public working drafts of its standards. Some important details remain to be filled in, and the Commission encourages all of the stakeholders to work within the W3C group to resolve these issues.

While more work remains to be done on Do Not Track, the Commission believes that the developments to date are significant and provide an effective path forward. The advertising industry, through the DAA, has committed to deploy browser-based technologies for consumer control over online tracking, alongside its ubiquitous icon program. The W3C process, thanks in part to the ongoing participation of DAA member companies, has made substantial progress toward specifying a consensus consumer choice system for tracking

254 Nick Wingfield, *Apple Adds Do-Not-Track Tool to New Browser*, Wall St. J. Apr. 13, 2011, *available at* http://online.wsj.com/article/SB10001424052748703551304576261272308358858.html.

255 *Comment of Google Inc.*, cmt. #00417, at 5.

256 Peter Kosmala, *Yes, Johnny Can Benefit From Transparency & Control*, Self-Regulatory Program for Online Behavioral Advertising, http://www.aboutads.info/blog/yes-johnny-can-benefit-transparency-and-control (Nov. 3, 2011); *see also* Press Release, Digital Advertising Alliance, White House, DOC and FTC Commend DAA's Self-Regulatory Program to Protect Consumers Online Privacy, (Feb. 23, 2012), *available at* http://www.aboutads.info/resource/download/DAA%20White%20House%20Event.pdf.

257 Digital Advertising Alliance, *About Self-Regulatory Principles for Multi-Site Data* (Nov. 2011), *available at* http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf.

258 Press Release, Digital Advertising Alliance, DAA Position on Browser Based Choice Mechanism (Feb. 22, 2012), *available at* http://www.aboutads.info/resource/download/DAA.Commitment.pdf.

that is practical and technically feasible.[259] The Commission anticipates continued progress in this area as the DAA members and other key stakeholders continue discussions within the W3C process to work to reach consensus on a Do Not Track system in the coming months.

d. Large Platform Providers That Can Comprehensively Collect Data Across the Internet Present Special Concerns.

As discussed above, even if a company has a first-party relationship with a consumer in one setting, this does not imply that the company can track the consumer for purposes inconsistent with the context of the interaction across the Internet, without providing choice. This principle applies fully to large platform providers such as ISPs, operating systems, and browsers, who have very broad access to a user's online activities.

For example, the preliminary staff report sought comment on the use of DPI for marketing purposes. Many commenters highlighted the comprehensive nature of DPI.[260] Because of the pervasive tracking that DPI allows, these commenters stated that its use for marketing should require consumers' affirmative express consent.[261] Privacy concerns led one commenter to urge the Commission to oppose DPI and hold workshops and hearings on the issue.[262] Another commenter argued that a lack of significant competition among broadband providers argues in favor of heightened requirements for consumer choice before ISPs can use DPI for marketing purposes.[263]

Two major ISPs emphasized that they do not use DPI for marketing purposes and would not do so without first seeking their customers' affirmative express consent.[264] They cautioned against singling out DPI as a practice that presents unique privacy concerns, arguing that doing so would unfairly favor certain technologies or business models at the expense of others. One commenter also stated that the framework should not favor companies that use other means of tracking consumers.[265] This commenter noted that various technologies – including cookies – allow companies to collect and use information in amounts similar to that made possible through DPI, and the framework's principles should apply consistently based

259 A system practical for both businesses and consumers would include, for users who choose to enable Do Not Track, significant controls on the collection and use of tracking data by third parties, with limited exceptions such as security and frequency capping. As noted above, first-party sharing with third parties is not consistent with the context of the interaction and would be subject to choice. Do Not Track is one way for users to express this choice.

260 *Comment of Computer and Communications Industry Ass'n*, cmt. #00233, at 15; *Comment of Center for Democracy & Technology*, cmt. #00469, at 14-15.

261 *See Comment of Center for Democracy & Technology*, cmt. #00469, at 14; *Comment of Phorm Inc.*, cmt. #00353, at 5; *see also Comment of Computer and Communications Industry Ass'n*, cmt. #00233, at 15 (urging that heightened requirements for consumer choice apply for the use of DPI); *Comment of Online Trust Alliance*, cmt. #00299, at 6 ("The use of DPI and related technologies may also be permissible when consumers have the ability to opt-in and receive appropriate and proportional quantifiable benefits in return.")

262 *Comment of Center for Digital Democracy and U.S. PIRG*, cmt. #00338, at 37.

263 *Comment of Computer and Communications Industry Ass'n*, cmt. #00233, at 15.

264 *Comment of AT&T Inc.*, cmt. #00420, at 21; *see also Comment of Verizon*, cmt. #00428, at 7 n.6. Likewise, a trade association of telecommunications companies represented that ISPs have not been extensively involved in online behavioral advertising. *See Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 33.

265 *See Comment of Verizon*, cmt. #00428, at 7.

on the type of information collected and how it is used.[266] Rather than isolating a specific technology, commenters urged the Commission to focus on the type of data collected and how it is used.[267]

ISPs serve as a major gateway to the Internet with access to vast amounts of unencrypted data that their customers send or receive over the ISP's network. ISPs are thus in a position to develop highly detailed and comprehensive profiles of their customers – and to do so in a manner that may be completely invisible. In addition, it may be difficult for some consumers to obtain alternative sources of broadband Internet access, and they may be inhibited from switching broadband providers for reasons such as inconvenience or expense. Accordingly, the Commission has strong concerns about the use of DPI for purposes inconsistent with an ISP's interaction with a consumer, without express affirmative consent or more robust protection.[268]

At the same time, the Commission agrees that any privacy framework should be technology neutral. ISPs are just one type of large platform provider that may have access to all or nearly all of a consumer's online activity. Like ISPs, operating systems and browsers may be in a position to track all, or virtually all, of a consumer's online activity to create highly detailed profiles.[269] Consumers, moreover, might have limited ability to block or control such tracking except by changing their operating system or browser.[270] Thus, comprehensive tracking by any such large platform provider may raise serious privacy concerns.

The Commission also recognizes that the use of cookies and social widgets to track consumers across unrelated websites may create similar privacy issues.[271] However, while companies such as Google and Facebook are expanding their reach rapidly, they currently are not so widespread that they could track a consumer's every movement across the Internet.[272] Accordingly, although tracking by these entities warrants consumer choice, the Commission does not believe that such tracking currently raises the same level of privacy concerns as those entities that can comprehensively track all or virtually of a consumer's online activity.

These are complex and rapidly evolving areas, and more work should be done to learn about the practices of all large platform providers, their technical capabilities with respect to consumer data, and their current and expected uses of such data. Accordingly, Commission staff will host a workshop in the second half

---

266 *Id.* at 7-8.

267 *See, e.g.*, *Comment of Internet Commerce Coalition*, cmt. #00447, at 10; *Comment of KINDSIGHT*, cmt. #00344, at 7-8 ; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 36; *Comment of Verizon*, cmt. #00428, at 7-8.

268 This discussion does not apply to ISPs' use of DPI for network management, security, or other purposes consistent with the context of a consumer's interaction with their ISP.

269 This discussion is not meant to imply that ISPs, operating systems, or browsers are currently building these profiles for marketing purposes.

270 ISPs, operating systems, and browsers have different access to users' online activity. A residential ISP can access unencrypted traffic from all devices currently located in the home. An operating system or browser, on the other hand, can access all traffic regardless of location and encryption, but only from devices on which the operating system or browser is installed. Desktop users have the ability to change browsers to avoid monitoring, but mobile users have fewer browser options.

271 A social widget is a button, box, or other possibly interactive display associated with a social network that is embedded into another party's website.

272 BrightEdge, *Social Share Report: Social Adoption Among Top Websites*, 3-4 (July 2011), *available at* http://www.brightedge.com/resfiles/brightedge-report-socialshare-2011-07.pdf (reporting that by mid-2011, the Facebook Like button appeared on almost 11% of top websites' front pages and Google's +1 button appeared on 4.5% of top websites' front pages); *see also* Justin Osofsky, *After f8: Personalized Social Plugins Now on 100,000+ Sites*, Facebook Developer Blog (May 11, 2010, 9:15 AM), http://developers.facebook.com/blog/post/382/.

of 2012 to explore the privacy issues raised by the collection and use of consumer information by a broad range of large platform providers such as ISPs, operating systems, browsers, search engines, and social media platforms as well as how competition issues may bear on appropriate privacy protection.[273]

e. Practices Requiring Affirmative Express Consent.

Numerous commenters focused on whether certain data collection and use practices warrant a heightened level of consent – *i.e.*, affirmative express consent.[274] These practices include (1) making material retroactive changes to a company's privacy representations; and (2) collection of sensitive data. These comments and the Commission's analysis are discussed here.

(i) Companies Should Obtain Affirmative Express Consent Before Making Material Retroactive Changes To Privacy Representations.

The preliminary staff report reaffirmed the Commission's bedrock principle that companies should provide prominent disclosures and obtain affirmative express consent before using data in a manner materially different than claimed at the time of collection.[275]

Although many commenters supported the affirmative express consent standard for material retroactive changes,[276] some companies called for an opt-out approach for material retroactive changes, particularly for changes that provide benefits to consumers.[277] One example cited was the development of Netflix's personalized video recommendation feature using information that Netflix originally collected in order to send consumers the videos they requested.[278] Other companies sought to scale the affirmative consent requirement according to the sensitivity of the data and whether the data is personally identifiable.[279] Many commenters sought clarification on when a change is material – for example, whether a change in data retention periods would be a material change requiring heightened consent.[280] One company posited

273 *See Comment of Center for Digital Democracy and U.S. PIRG*, cmt. #00338, at 37 (recommending FTC hold a workshop to address DPI).

274 Companies may seek "affirmative express consent" from consumers by presenting them with a clear and prominent disclosure, followed by the ability to opt in to the practice being described. Thus, for example, requiring the consumer to scroll through a ten-page disclosure and click on an "I accept" button would not constitute affirmative express consent.

275 In the preliminary report, this principle appeared under the heading of "transparency." *See, e.g., In the Matter of Gateway Learning Corp.*, FTC Docket No. C-4120 (Sept. 10, 2004) (consent order) (alleging that Gateway violated the FTC Act by applying material changes to a privacy policy retroactively), *available at* http://www.ftc.gov/os/caselist/0423047/040917do0423047.pdf; *see also* FTC, *Self-Regulatory Principles for Online Behavioral Advertising* (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf (noting the requirement that companies obtain affirmative express consent before making material retroactive changes to their privacy policies).

276 *See Comment of Consumers Union*, cmt. #00362, at 17; *Comment of Future of Privacy Forum*, cmt. #00341, at 5; *Comment of Privacy Rights Clearinghouse*, cmt. #00351, at 21.

277 *See Comment of Facebook, Inc.*, cmt. #00413, at 11; *see also Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 12; *Comment of AT&T Inc.*, cmt. #00420, at 29-30; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 30-31.

278 *Comment of Facebook, Inc.*, cmt. #00413, at 8.

279 *See Comment of AT&T Inc.*, cmt. #00420, at 30; *Comment of Phorm Inc.*, cmt. #00353, at 1.

280 *See Comment of Future of Privacy Forum*, cmt. #00341, at 4; *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 12; *Comment of Microsoft Corp.*, cmt. #00395, at 17.

that the affirmative express consent standard would encourage vague disclosures at the outset to avoid the requirement for obtaining such consent.[281]

The Commission reaffirms its commitment to requiring companies to give prominent disclosures and to obtain express affirmative consent for material retroactive changes. Indeed, the Commission recently confirmed this approach in its settlements with Google and Facebook. The settlement agreements mandate that the companies give their users clear and prominent notice and obtain affirmative express consent prior to making certain material retroactive changes to their privacy practices.[282]

In response to the request for clarification on what constitutes a material change, the Commission notes that, at a minimum, sharing consumer information with third parties after committing at the time of collection not to share the data would constitute a material change. There may be other circumstances in which a change would be material, which would have to be determined on a case-by-case basis, analyzing the context of the consumer's interaction with the business.

The Commission further notes that commenters' concerns that the affirmative express consent requirement would encourage vague disclosures at the outset should be addressed by other elements of the framework. For example, other elements of the framework call on companies to improve and standardize their privacy statements so that consumers can easily glean and compare information about various companies' data practices. The framework also calls on companies to give consumers specific information and choice at a time and in a context that is meaningful to consumers. These elements, taken together, are intended to result in disclosures that are specific enough to be meaningful to consumers.

The preliminary staff report posed a question about the appropriate level of consent for prospective changes to companies' data collection and use. One commenter cited the rollout of Twitter's new user interface – "new Twitter" – as a positive example of a set of prospective changes about which consumers received ample and adequate notice and ability to exercise choice.[283] When "new Twitter" was introduced, consumers were given the opportunity to switch to or try out the new interface, or to keep their traditional Twitter profile. The Commission supports innovative efforts such as these to provide consumers with meaningful choices when a company proposes to change its privacy practices on a prospective basis.

(ii) Companies Should Obtain Consumers' Affirmative Express Consent Before Collecting Sensitive Data.

A variety of commenters discussed how to delineate which types of data should be considered sensitive. These comments reflect a general consensus that information about children, financial and health information, Social Security numbers, and precise, individualized geolocation data is sensitive and

281 *Comment of Facebook, Inc.*, cmt. #00413, at 10.

282 *See In the Matter of Google Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf; *In the Matter of Facebook, Inc.*, FTC File No. 092-3184 (Nov. 29, 2011) (proposed consent order), *available at* http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.

283 *Comment of Electronic Frontier Foundation*, cmt. #00400, at 15.

merits heightened consent methods.[284] In addition, some commenters suggested that information related to race, religious beliefs, ethnicity, or sexual orientation, as well as biometric and genetic data, constitute sensitive data.[285] One commenter also characterized as sensitive information about consumers' online communications or reading and viewing habits.[286] Other commenters, however, noted the inherent subjectivity of the question and one raised concerns about the effects on market research if the definition of sensitive data is construed too broadly.[287]

Several commenters focused on the collection and use of information from teens, an audience that may be particularly vulnerable. A diverse coalition of consumer advocates and others supported heightened protections for teens between the ages of 13 and 17.[288] These commenters noted that while teens are heavy Internet users, they often fail to comprehend the long-term consequences of sharing their personal data. In order to better protect this audience, the commenters suggested, for example, limiting the amount of data that websites aimed at teens can collect or restricting the ability of teens to share their data widely through social media services.

Conversely, a number of industry representatives and privacy advocates objected to the establishment of different rules for teens.[289] These commenters cited the practical difficulties of age verification and the potential that content providers will simply elect to bar teen audiences.[290] Rather than requiring different choice mechanisms for this group, one company encouraged the FTC to explore educational efforts to address issues that are unique to teens.[291]

Given the general consensus regarding information about children, financial and health information, Social Security numbers, and precise geolocation data, the Commission agrees that these categories of information are sensitive. Accordingly, before collecting such data, companies should first obtain affirmative express consent from consumers. As explained above, the Commission also believes that companies should

284 *See, e.g., Comment of Consumer Federation of America*, cmt. #00358, at 9; *Comment of CNIL*, cmt. #00298, at 4; *Comment of Massachusetts Office of the Attorney General*, cmt. #00429, at 3; *Comment of Kindsight*, cmt. #00344, at 11; *Comment of Experian*, cmt. #00398, at 9; *Comment of Center for Democracy & Technology*, cmt. #00469, at 14; *Comment of Office of the Information and Privacy Commissioner of Ontario*, cmt. #00239, at 2; *see also Comment of TRUSTe*, cmt. #00450, at 11 (agreeing that sensitive information should be defined to include information about children, financial and medical information, and precise geolocation information but urging that sensitive information be more broadly defined as "information whose unauthorized disclosure or use can cause financial, physical, or reputational harm"); *Comment of Facebook, Inc.*, cmt. #00413, at 23 (agreeing that sensitive information may warrant enhanced consent, but noting that enhanced consent may not be possible for activities such as the posting of status updates by users where those updates may include sensitive information such as references to an illness or medical condition).

285 *See Comment of Consumer Federation of America*, cmt. #00358, at 9; *see also Comment of CNIL*, cmt. #00298, at 4, *Comment of Center for Digital Democracy and U.S. PIRG*, cmt. #00338, at 35.

286 *See Comment of Electronic Frontier Foundation*, cmt. #00400, at 7.

287 *See Comment of Marketing Research Ass'n*, cmt. #00405, at 6-7; *Comment of American Trucking Ass'ns*, cmt. #00368, at 2-3; *Comment of Microsoft Corp.*, cmt. #00395, at 10.

288 *See Comment of Institute for Public Representation*, cmt. #00346, at 4; *Comment of Consumers Union*, cmt. #00362, at 13.

289 *See Comment of Center for Democracy & Technology*, cmt. #00469, at 15; *Comment of CTIA – The Wireless Ass'n*, cmt. #00375, at 12-13; *Comment of Microsoft Corp.*, cmt. #00395, at 10; *see also Comment of Electronic Frontier Foundation*, cmt. #00400, at 14 (opposing the creation of special rules giving parents access to data collected about their teenaged children); *Comment of PrivacyActivism*, cmt. #00407, at 4 (opposing the creation of special rules giving parents access to data collected about their teenaged children).

290 *See Comment of Center for Democracy & Technology*, cmt. #00469, at 15; *Comment of CTIA – The Wireless Ass'n*, cmt. #00375, at 12-13; *Comment of Microsoft Corp.*, cmt. #00395, at 10.

291 *See Comment of Microsoft Corp.*, cmt. #00395, at 10.

follow this practice irrespective of whether they use the sensitive data for first-party marketing or share it with third parties.[292]

The Commission is cognizant, however, that whether a particular piece of data is sensitive may lie in the "eye of the beholder" and may depend upon a number of subjective considerations. In order to minimize the potential of collecting any data – whether generally recognized as sensitive or not – in ways that consumers do not want, companies should implement *all* of the framework's components. In particular, a consumer's ability to access – and in appropriate cases to correct or delete – data will allow the consumer to protect herself when she believes the data is sensitive but others may disagree.

With respect to whether information about teens is sensitive, despite the difficulties of age verification and other concerns cited in the comments, the Commission agrees that companies that target teens should consider additional protections. Although affirmative express consent may not be necessary in every advertising campaign directed to teens, other protections may be appropriate. For example, all companies should consider shorter retention periods for teens' data.

In addition, the Commission believes that social networking sites should consider implementing more privacy-protective default settings for teens. While some teens may circumvent these protections, they can function as an effective "speed bump" for this audience and, at the same time, provide an opportunity to better educate teens about the consequences of sharing their personal information. The Commission also supports access and deletion rights for teens, as discussed below.[293]

Final Principle: For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data. Companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes.

D. TRANSPARENCY

Baseline Principle: Companies should increase the transparency of their data practices.

Citing consumers' lack of awareness of how, and for what purposes, companies collect, use, and share data, the preliminary staff report called on companies to improve the transparency of their data practices. Commission staff outlined a number of measures to achieve this goal. One key proposal, discussed in the previous section, is to present choices to consumers in a prominent, relevant, and easily accessible place at a time and in a context when it matters to them. In addition, Commission staff called on industry to make privacy statements clearer, shorter, and more standardized; give consumers reasonable access to their data; and undertake consumer education efforts to improve consumers' understanding of how companies collect, use, and share their data.

292 *See infra* at Section IV.C.1.b.(v).

293 *See infra* at Section IV.D.2.b.

research underway in this area.[300] Another suggested the "form builder" approach used for GLBA Short Notices to standardize the format of privacy notices outside the financial context.[301] One consumer group called for standardization of specific terms like "affiliate" and "anonymize" so that companies' descriptions of their data practices are more meaningful.[302] A wide range of commenters suggested that different industry sectors come together to develop standard privacy notices.[303] Other commenters opposed the idea of mandated standardized notices, arguing that the Commission should require only that privacy statements be clear and in plain language. These commenters stated that privacy statements need to take into account differences among business models and industry sectors.[304]

Privacy statements should account for variations in business models across different industry sectors, and prescribing a rigid format for use across all sectors is not appropriate. Nevertheless, the Commission believes that privacy statements should contain some standardized elements, such as format and terminology, to allow consumers to compare the privacy practices of different companies and to encourage companies to compete on privacy. Accordingly, Commission calls on industry sectors to come together to develop standard formats and terminology for privacy statements applicable to their particular industries. The Department of Commerce will convene multi-stakeholder groups to work on privacy issues; this could be a useful venue in which industry sectors could begin the exercise of developing more standardized, streamlined privacy policies.

Machine-readable policies,[305] icons, and other alternative forms of providing notice also show promise as tools to give consumers the ability to compare privacy practices among different companies.[306] In response to the preliminary staff report's question on machine-readable policies, commenters agreed that such policies could improve transparency.[307] One commenter proposed combining the use of machine-readable policies with icons and standardized policy statements (*e.g.*, "we collect but do not share consumer data

300 *See Comment of Consumer Watchdog*, cmt. #00402, at 2; *Comment of Consumer Federation of America*, cmt. #00358, at 16; *see also Comment of Lorrie Faith Cranor*, cmt. #00453, at 2 n.7 (discussing P3P authorizing tools that enable automatic generation of "nutrition label" privacy notices).

301 *See Comment of Privacy Rights Clearinghouse*, cmt. #00351, at 16.

302 *See Comment of Electronic Frontier Foundation*, cmt. #00400, at 6.

303 *See Comment of General Electric*, cmt. #00392, at 2; *Comment of the Information Commissioner's Office of the UK*, cmt. #00249, at 4; *Comment of Consumers Union*, cmt. #00362, at 15-16; *Comment of Facebook, Inc.*, cmt. #00413, at 9.

304 *See Comment of AT&T Inc.*, cmt. #00420, at 25; *Comment of eBay*, cmt. #00374, at 10; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 29; *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 12; *Comment of Microsoft Corp.*, cmt. #00395, at 15.

305 A machine-readable privacy policy is a statement about a website's privacy practices – such as the collection and use of data – written in a standard computer language (not English text) that software tools such as consumer's web browser can read automatically. For example, when the browser reads a machine-readable policy, the browser can compare the policy to the consumer's browser privacy preferences, and can inform the consumer when these preferences do not match the practices of the website he is visiting. If the consumer decides he does not want to visit websites that sell information to third parties, he might set up a rule that recognizes that policy and blocks such sites or display a warning upon visiting such a site. Machine-readable language will be the subject of an upcoming summit. *See* White House, National Archives & Records Administration, *Informing Consumers Through Smart Disclosures* (Mar. 1, 2012), *available at* http://www.nist.gov/ineap/upload/Summit_Invitation_to_Agencies_FINAL.pdf (describing upcoming summit).

306 Likewise, new tools like privacyscore.com may help consumers more readily compare websites' data practices. *See* Tanzina Vega, *A New Tool in Protecting Online Privacy*, N.Y. Times, Feb. 12, 2012, *available at* http://mediadecoder.blogs.nytimes.com/2012/02/12/a-new-tool-in-protecting-online-privacy/?scp=2&sq=privacy&st=cse.

307 *Comment of Phorm Inc.*, cmt. #00353, at 9; *Comment of Lorrie Faith Cranor*, cmt. #00453, at 6.

Commenters offered proposals for how to achieve greater transparency and sought clarification on how they should implement these elements of the framework. Although the Commission adopts the proposed framework's transparency principle without change, it clarifies the application of the framework in response to these comments, as discussed below.

1. PRIVACY NOTICES

Proposed Principle: Privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices.

The preliminary staff report highlighted the consensus among roundtable participants that most privacy policies are generally ineffective for informing consumers about a company's data practices because they are too long, are difficult to comprehend, and lack uniformity.[294] While acknowledging privacy policies' current deficiencies, many roundtable participants agreed that the policies still have value – they provide an important accountability function by educating consumer advocates, regulators, the media, and other interested parties about the companies' data practices.[295] Accordingly, Commission staff called on companies to provide clear and concise descriptions of their data collection and use practices. Staff further called on companies to standardize the format and the terminology used in privacy statements so that consumers can compare the data practices of different companies and exercise choices based on privacy concerns, thereby encouraging companies to compete on privacy.

Despite the consensus from the roundtables that privacy statements are not effective at communicating a company's data collection and use practices to consumers, one commenter disagreed that privacy notices need to be improved.[296] Another commenter pointed out that providing more granular information about data collection and use practices could actually increase consumer confusion by overloading the consumer with information.[297] Other industry commenters highlighted the work they have undertaken since the preliminary staff report to improve their own privacy statements.[298]

Many consumer groups supported staff's call to standardize the format and terminology used in privacy statements so that consumers could more easily compare the practices of different companies.[299] Some commenters suggested a "nutrition label" approach for standardizing the format of privacy policies and cited

294 Recent research and surveys suggests that many consumers (particularly among lower income brackets and education levels) do not read or understand privacy policies, thus further heightening the need to make them more comprehensible. Notably, in a survey conducted by Zogby International, 93% of adults – and 81% of teens – indicated they would take more time to read terms and conditions for websites if they were shorter and written in clearer language. *See Comment of Common Sense Media*, cmt. #00457, at 1.

295 *See Comment of AT&T, Inc.*, cmt. #00420, at 17; *Comment of Center for Democracy & Technology*, cmt. #00469, at 24.

296 *See Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 22.

297 *See Comment of United States Council for International Business*, cmt. #00366, at 3.

298 *See Comment of Google Inc.*, cmt. #00417, at 1; *Comment of Facebook, Inc.*, cmt. #00413, at 9; *Comment of AT&T Inc.*, cmt. #00420, at 24.

299 *See Comment of Privacy Rights Clearinghouse*, cmt. #00351, at 15-16; *Comment of Consumer Federation of America*, cmt. #00358, at 16; *Comment of Consumer Watchdog*, cmt. #00402, at 2.

on mobile screens. These factors increase the urgency for the companies providing mobile services to come together and develop standard notices, icons, and other means that the range of businesses can use to communicate with consumers in a consistent and clear way.

To address this issue, the Commission notes that it is currently engaged in a project to update its existing business guidance about online advertising disclosures.[317] In conjunction with this project, Commission staff will host a workshop later this year.[318] One of the topics to be addressed is mobile privacy disclosures: How can these disclosures be short, effective, and accessible to consumers on small screens? The Commission hopes that the discussions at the workshop will spur further industry self-regulation in this area.

Final Principle: Privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices.

2. ACCESS

Proposed Principle: Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use.

There was broad agreement among a range of commenters that consumers should have some form of access to their data. Many of these commenters called for flexibility, however, and requested that access rights be tiered according to the sensitivity and intended use of the data at issue.[319] One commenter argued that access rights should be limited to sensitive data, such as financial account information, because a broader access right would be too costly for offline retailers.[320] Some companies and industry representatives supported providing consumers full access to data that is used to deny benefits; several commenters affirmed the significance of the FCRA in providing access to information used for critical decisionmaking. For other less sensitive data, such as marketing data, they supported giving consumers a general notice describing the types of data they collect and the ability to suppress use of the data for future marketing.[321]

One commenter raised concerns about granting access and correction rights to data files used to prevent fraudulent activity, noting that such rights would create risks of fraud and identity theft. This commenter also stated that companies would need to add sensitive identifying information to their marketing databases in order to authenticate a consumer's request for information, and that the integration of multiple databases would raise additional privacy and security risks.[322]

317 *See* Press Release, FTC, FTC Seeks Input to Revising its Guidance to Business About Disclosures in Online Advertising (May 26, 2011), *available at* http://www.ftc.gov/opa/2011/05/dotcom.shtm.

318 *See* Press Release, FTC, FTC Will Host Public Workshop to Explore Advertising Disclosures in Online and Mobile Media on May 30, 2012 (Feb. 29, 2012), *available at* http://www.ftc.gov/opa/2012/02/dotcom.shtm.

319 *Comment of Intuit, Inc.*, cmt. #00348, at 12; *Comment of eBay*, cmt. #00374, at 10; *Comment of IBM*, cmt. #00433, at 3; *Comment of Consumers Union*, cmt. #00362, at 16.

320 *Comment of Meijer*, cmt. #00416, at 7.

321 *Comment of Intel Corp.*, cmt. #00246, at 8; *Comment of The Centre for Information Policy Leadership at Hunton & Williams LLP*, cmt. #00360, at 8; *Comment of Experian*, cmt. #00398, at 11.

322 *Comment of Experian*, cmt. #00398, at 10-11.

with third parties") to simplify privacy decision-making for consumers.[308] Other commenters described how icons work or might work in different business contexts. One browser company described efforts underway to develop icons that might be used to convey information, such as whether a consumer's data is sold or may be subject to secondary uses, in a variety of business contexts.[309] Representatives from online behavioral advertising industry groups also described their steps in developing and implementing an icon to communicate that online behavioral advertising may be taking place.[310]

Commenters also discussed the particular challenges associated with providing notice in the mobile context, noting the value of icons, summaries, FAQs, and videos.[311] Indeed, some work already has been done in this area to increase the transparency of data practices. For example, the advocacy organization Common Sense Media reviews and rates mobile apps based on a variety of factors including privacy[312] and a platform provider uses an icon to signal to consumers when a mobile application is using location information.[313] In addition, CTIA – a wireless industry trade group – in conjunction with the Entertainment Software Rating Board, recently announced plans to release a new rating system for mobile apps.[314] This rating system, which is based on the video game industry's model, will use icons to indicate whether specific apps are appropriate for "all ages," "teen," or only "adult" audiences. The icons will also detail whether the app shares consumers' personal information. Noting the complexity of the mobile ecosystem, which includes device manufacturers, operating system providers, mobile application developers, and wireless carriers, some commenters called for public workshops to bring together different stakeholders to develop a uniform approach to icons and other methods of providing notice.[315] Also, as noted above, the Mobile Marketing Association has released its Mobile Application Privacy Policy.[316]

The Commission appreciates the complexities of the mobile environment, given the multitude of different entities that want to collect and use consumer data and the small space available for disclosures

308 *Comment of Lorrie Faith Cranor*, cmt. #00453, at 6 (explaining how icons combined with standard policies might work: "For example, a type I policy might commit to not collecting sensitive categories of information and not sharing personal data except with a company's agents, while a type II policy might allow collection of sensitive information but still commit to not sharing them, a type III policy might share non-identified information for behavioral advertising, and so on. Companies would choose which policy type to commit to. They could advertise their policy type with an associated standard icon, while also providing a more detailed policy. Users would be able to quickly determine the policy for the companies they interact with.").

309 *Comment of Mozilla*, cmt. #00480, at 12.

310 *Comment of American Ass'n of Advertising Agencies, American Advertising Federation, Ass'n of National Advertisers, Direct Marketing Ass'n, Inc., and Interactive Advertising Bureau*, cmt. #00410 at 2-3; *Comment of Digital Marketing Alliance*, cmt. #00449, at 18-24; *Comment of Evidon*, cmt. #00391, at 3-6; *Comment of Internet Advertising Bureau*, cmt. #00388, at 4.

311 *Comment of General Electric*, cmt. #00392, at 1-2; *Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 2-3; *Comment of Mozilla*, cmt. #00480, at 12.

312 *See* Common Sense Media, App Reviews, http://www.commonsensemedia.org/app-reviews.

313 *See* Letter from Bruce Sewell, General Counsel & Senior Vice President of Legal and Governmental Affairs, Apple, to Hon. Edward J. Markey, U.S. House of Representatives (May 6, 2011), *available at* http://robert.accettura.com/wp-content/uploads/2011/05/apple_letter_to_ejm_05.06.11.pdf.

314 *See* Press Release, CTIA – The Wireless Ass'n, CTIA – The Wireless Ass'n to Announce Mobile Application Rating System with ESRB (Nov. 21, 2011), *available at* http://www.ctia.org/media/press/body.cfm/prid/2145.

315 *Comment of Consumer Federation of America*, cmt. #00358, at 16; *Comment of GSMA*, cmt. #00336, at 10.

316 Although this effort is promising, more work remains. The Mobile Marketing Association's guidelines are not mandatory and there is little recourse against companies who elect not to follow them. More generally, there are too few players in the mobile ecosystem who are committed to self-regulatory principles and providing meaningful disclosures and choices.

A number of commenters raised issues about the costs associated with providing access. One company suggested that access rights be flexible, taking into account the company's existing data infrastructure.[323] Others argued that access be granted only to consumer information that is "reasonably accessible in the course of business"[324] and one commenter said that companies should be able to charge for providing access where there are costs associated with retrieving and presenting data.[325]

Commenters also asserted that companies should tell consumers the entities with which their data has been shared.[326] Citing California's "Shine the Light" law, one commenter stated that companies should not only identify the third parties with which they share consumer data but should also disclose how the third parties use the data for marketing.[327] Another commenter pointed out that many marketers do not maintain records about data sold to other companies on an individual basis. Thus, marketers have the ability to identify the companies to which they have sold consumer data in general, but not the third parties with which they may have shared the information about any individual consumer.[328]

Some comments reflect support for requiring companies to identify for consumers the sources of data collected about them so that consumers can correct erroneous data at the source, if appropriate.[329] One commenter noted that the DMA self-regulatory guidelines currently require that a marketer identify the sources of data maintained about consumers.[330]

The Commission agrees with the commenters who stated that consumer access should be proportional to the sensitivity and the intended use of the data at issue. Indeed, the comments generally support treating access in accordance with three categories that reflect different levels of data sensitivity: (1) entities that maintain data for marketing purposes; (2) entities subject to the FCRA; and (3) entities that may maintain data for other, non-marketing purposes that fall outside of the FCRA.

At one side of the spectrum are companies that maintain data for marketing purposes. For data used solely for marketing purposes, the Commission agrees with the commenters who stated that the costs of providing individualized access and correction rights would likely outweigh the benefits. The Commission continues to support the idea of businesses providing consumers with access to a list of the categories of consumer data they hold, and the ability to suppress the use of such data for marketing. This approach

323 *Comment of AT&T Inc.*, cmt. #00420, at 28-29.

324 *Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 3; *Comment of Yahoo!, Inc.*, cmt. #00444, at 20; *Comment of The Centre for Information Policy Leadership at Hunton & Williams LLP*, cmt. #00360, at 5-6.

325 *Comment of U.S. Council for International Business*, cmt. #00366, at 3.

326 *Comment of Catalog Choice*, cmt. #00473, at 8-9; *Comment of the Information Commissioner's Office of the UK*, cmt. #00249, at 5.

327 *See Comment of Catalog Choice*, cmt. #00473, at 20. Under this law, businesses, upon request, must provide their customers, free of charge and within 30 days: (1) a list of the categories of personal information disclosed by the business to third parties for the third parties' marketing purposes, (2) the names and addresses of all of the third parties that received personal information from the business in the preceding calendar year, (3) and if the nature of the third parties's business cannot reasonably be determined from the third parties' name, examples of the products or services marketed by the third party. Cal. Civ. Code § 1798.83.

328 *Comment of The Centre for Information Policy Leadership at Hunton & Williams, LLP*, cmt. #00360, at 7.

329 *Comment of Reputation.com, Inc.*, cmt. #00385, at 11-12; *see also Comment of Center for Democracy & Technology*, cmt. #00469, at 25.

330 *Comment of The Centre for Information Policy Leadership at Hunton & Williams, LLP*, cmt. #00360, at 7.

will provide consumers with an important transparency tool without imposing significant new costs for businesses.[331]

The Commission does, however, encourage companies that maintain consumer data for marketing purposes to provide more individualized access when feasible. One example of an innovation in this area is the advertising preference managers that companies such as Google and Yahoo! have implemented. Yahoo!, for example, offers consumers, through its Ad Interest Manager, the ability to access the specific interest categories that Yahoo! associates with individual consumers and allows them to suppress marketing based on some or all of these categories. Using this service, an elementary school teacher who conducted online research for pet food during the time she owned a dog, but continues to receive advertisements for dog food, could remove herself from the "Consumer Packaged Goods > Pets and Animals > Food and Supplies" category while still opting to remain part of the "Life Stages > Education > K to 12" category.[332] The Commission supports efforts by companies to provide consumers with these types of granular choices to give them greater control over the marketing materials and solicitations they receive.

At the other end of the spectrum are companies that assemble and evaluate consumer information for use by creditors, employers, insurance companies, landlords, and other entities involved in eligibility decisions affecting consumers. The preliminary staff report cited the FCRA as an important tool that provides consumers with the right to access their own data that has been used to make such decisions, and if it is erroneous, to correct it. Several commenters echoed this view.[333]

The FCRA recognizes the sensitivity of the data that consumer reporting agencies maintain and the ways in which various entities use it to evaluate whether a consumer is able to participate in so many activities central to modern life; therefore, it provides consumers with access and correction rights for information contained in consumer reports. Pursuant to the FCRA, consumer reporting agencies are required to disclose to consumers, upon request, all items in the consumer's file, no matter how or where they are stored, as well as the entities with which the consumer reporting agency shared the information in a consumer's report. When consumers identify information in their report that is incomplete or inaccurate, and report it to a consumer reporting agency, the agency must investigate and correct or delete such information in certain circumstances.

As more and more consumer data becomes available from a variety of sources, companies are increasingly finding new opportunities to compile, package, and sell that information. In some instances, companies could be compiling and selling this data to those who are making decisions about a consumer's eligibility for credit, insurance, employment, and the like. To the extent companies are assembling data and marketing or selling it for such purposes, they are subject to the FCRA. For example, companies that compile social media information and provide it to employers for use in making hiring decisions are consumer reporting

331 As discussed above, in most cases the framework does not require companies to provide consumer choice for first-party marketing, although first parties may choose to provide such choice to meet consumer demand. Outside of the first-party marketing context, however, companies should provide consumers with the ability to suppress the use of their data for marketing.

332 *See* Yahoo!, Ad Interest Manager, http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting.

333 *Comment of Consumer Data Industry Ass'n*, cmt. #00363, at 4 - 5; *Comment of Experian*, cmt. #00398, at 10.

Should cos get your college debt off when picking your salary?

agencies and thus required to provide consumers with access and correction rights under the FCRA.[334] These companies would also be required to inform employers about their FCRA obligation to provide adverse action notices when, for example, employment is denied.

Even if a company is not compiling and sharing data for the specific purpose of making employment, credit, or insurance eligibility decisions, if the company has reason to believe the data will be used for such purposes, it would still be covered by the FCRA. For example, recently, the Commission issued warning letters to the developers of mobile apps that compiled public record information on individuals and created apps for the purposes of learning information about friends, co-workers, neighbors, or potential suitors.[335] The Commission noted that if these apps marketed their services for employment purposes or otherwise had reason to believe that they were being used for employment purposes, the FCRA requirements would apply.

Finally, some businesses may maintain and use consumer data for purposes that do not fall neatly within either the FCRA or marketing categories discussed above. These businesses may encompass a diverse range of industry sectors. They may include businesses selling fraud prevention or risk management services, in order to verify the identities of customers. They may also include general search engines, media publications, or social networking sites. They may include debt collectors trying to collect a debt. They may also include companies collecting data about how likely a consumer is to take his or her medication, for use by health care providers in developing treatment plans.[336]

For these entities, the Commission supports the sliding scale approach, which several commenters endorsed,[337] with the consumer's ability to access his or her own data scaled to the use and sensitivity of the data. At a minimum, these entities should offer consumers access to (1) the types of information the companies maintain about them;[338] and (2) the sources of such information.[339] The Commission believes that requiring companies to identify data sources would help consumers to correct erroneous information at the source. In appropriate circumstances the Commission urges companies to provide the names of the third parties with whom consumer information is shared.

In instances where data is more sensitive or may affect benefits, more individualized notice, access, and correction rights may be warranted. For example, if a company denies services to a consumer because it could not verify the consumer's identity, it may be appropriate for the company to disclose the name of the identity verification service used. This will allow the consumer to contact the data source, which can then provide the consumer with access to the underlying information, as well as any appropriate remedies, such

334 15 U.S.C. §§ 1681g-1681h. *See* Letter from Maneesha Mithal, Assoc. Dir., Div. of Privacy and Identity Prot., FTC, to Renee Jackson, Counsel for Social Intelligence Corp., (May 9, 2011) (closing letter), *available at* http://www.ftc.gov/os/closings/110509socialintelligenceletter.pdf .

335 *See* Press Release, FTC, FTC Warns Marketers That Mobile Apps May Violate Fair Credit Reporting Act (Feb. 7, 2012), *available at* http://www.ftc.gov/opa/2012/02/mobileapps.shtm (describing warning letters sent by the FTC to Everify, Inc., InfoPay, Inc., and Intelligator, Inc. on Jan. 25, 2012).

336 *See* Laura Landro, *Many Pills, Many Not Taken*, WALL ST. J., Oct. 10, 2011, *available at* http://online.wsj.com/article/SB10001424052970203388804576616882856318782.html.

337 *Comment of Consumers Union*, cmt. #00362, at 16; *Comment of CTIA – The Wireless Ass'n*, cmt. #00375, at 7; *Comment of Microsoft Corp.*, cmt. #00395, at 15-16.

338 *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at Ex. A.

339 *Comment of Reputation.com, Inc.*, cmt. #00385, at 11-12. Of course, First Amendment protections would apply to journalists' sources, among other things, and the Commission's recommendations are not intended to apply in that area.

as the ability to correct the information.[340] To ensure that the consumer knows that she has been denied a benefit based on her own data, as a best practice the company should notify the consumer of the denial and the information on which the denial was based.

Verifying the identity of users who seek access to their own information is an important consideration and should be approached from a risk management perspective, focusing on the likelihood of and potential harm from misidentification. Indeed, in the example of identity verification services described above, one would not want a criminal to be able to "correct" his or her own truthful data, and it would be appropriate to require somewhat more stringent safeguards and proof of identity before allowing access and correction. Certainly, consumer reporting agencies have developed procedures allowing them to verify the identity of requesting consumers using the multiple pieces of information they have about consumers to match information provided by the requesting consumer. Companies engaged in providing data for making eligibility determinations should develop best practices for authenticating consumers for access purposes.

On the other hand, the significantly reduced risks associated with providing the wrong person's information contained in a marketing database that contains no sensitive information may justify less stringent authentication procedures.[341] As with other issues discussed in this Report, reasonableness should be the touchstone: the degree of authentication employed should be tied to the sensitivity of the information maintained and how such information is used.

a. Special Access Mechanism for Data Brokers

Data brokers are companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers for various purposes, including verifying an individual's identity, differentiating records, marketing products, and preventing financial fraud. Several commenters noted the lack of transparency about the practices of these entities, which often have a wealth of information about consumers but never interact directly with them.[342] Consumers are often unaware of the existence of these entities, as well as the purposes for which they collect and use data.[343] One commenter noted that data brokers may sell data to employers, background screeners, and law enforcement, among others, without the consumer's knowledge.[344] The Commission has monitored data brokers since the 1990s, hosting workshops, drafting reports, and testifying before Congress about

340 As noted above, companies should pay close attention to the types of eligibility determinations being made to ensure they comply with the FCRA, if warranted.

341 One commenter noted that when organizations collect and maintain sensitive information about individuals, such as for banking or issuance of credit, they will ask for authenticating information before an individual can access those records. This same commenter then stated that organizations holding less sensitive data may not require similarly rigorous authentication. *See Comment of The Centre for Information Policy Leadership at Hunton & Williams, LLP*, cmt. #00360, at 7 n.6.

342 *See Comment of Privacy Rights Clearinghouse*, cmt. #00351, at 3; *Comment of Consumers Union*, cmt. #00362, at 11.

343 *See Comment of Consumer Federation of America*, cmt. #00358, at 17.

344 *See Comment of Privacy Rights Clearinghouse*, cmt. #00351, at 8.

What are they exactly?

the privacy implications of data brokers' practices.[345] Following a Commission workshop, the data broker industry created the Individual References Services Group (IRSG), a self-regulatory organization for certain data brokers.[346] Although industry ultimately terminated this organization, a series of public breaches – including one involving ChoicePoint – led to renewed scrutiny of the practices of data brokers.[347] And, indeed, there have been few broad-based efforts to implement self-regulation in this area in the recent past.

The access rights discussed above will help to improve the transparency of companies' data practices generally, whether or not they have a direct consumer interface. Because most data brokers are invisible to consumers, however, the Commission makes two additional recommendations as to these entities.

First, since 2009, the Commission has supported legislation giving access rights to consumers for information held by data brokers. During the 111th Congress, the House approved a bill that included provisions to establish a procedure for consumers to access information held by data brokers.[348] To improve the transparency of this industry's practices, the Commission has testified in support of the goals of this legislation[349] and continues to support legislation in this area.[350]

Second, the Commission recommends that the data broker industry explore the idea of creating a centralized website where data brokers that compile and sell data for marketing could identify themselves to consumers and describe how they collect consumer data and disclose the types of companies to which they sell the information. Additionally, data brokers could use the website to explain the access rights and other choices they offer consumers, and could offer links to their own sites where consumers could exercise such options.[351] This website will improve transparency and give consumers control over the data practices of companies that maintain and share data about them for marketing purposes. It can also provide consumer-facing entities such as retailers a means for ensuring that the information brokers from which they purchase "enhancement" information have instituted appropriate transparency and control mechanisms. Indeed, the

345 *See, e.g.*, Prepared Statement of the FTC, *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information: Hearing Before the Senate Comm. on Banking, Housing, and Urban Affairs*, 109th Cong. (Mar. 10, 2005), *available at* http://www.ftc.gov/os/testimony/050310idtheft.pdf; *see also* FTC Workshop, *The Information Marketplace: Merging & Exchanging Consumer Data* (Mar. 13, 2001), *available at* http://www.ftc.gov/bcp/workshops/infomktplace/index.shtml; FTC Workshop, *Information Flows: The Costs and Benefits to Consumers and Businesses of the Collection and Use of Consumer Information* (June 18, 2003), *available at* http://www.ftc.gov/bcp/workshops/infoflows/030618agenda.shtm.

346 *See* FTC, *Individual Reference Services, A Report to Congress* (1997), *available at* http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm.

347 *See* Prepared Statement of the FTC, *Protecting Consumers' Data: Policy Issues Raised by ChoicePoint: Hearing before H. Comm. on Energy and Commerce, Subcomm. on Commerce, Trade, and Consumer Protection, Comm. on Energy and Commerce*, 109th Cong. (Mar. 15, 2005), *available at* http://www.ftc.gov/os/2005/03/050315protectingconsumerdata.pdf.

348 Data Accountability and Trust Act, H.R. 2221, 111th Congress (as passed by House, Dec. 8, 2009).

349 *See, e.g.*, Prepared Statement of the FTC, *Legislative Hearing on H.R. 2221, the Data Accountability and Protection Act, and H.R. 1319, the Informed P2P User Act: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Trade, and Consumer Protection*, 111th Cong. (May 5, 2009), *available at* http://www.ftc.gov/os/2009/05/P064504peertopeertestimony.pdf.

350 *See, e.g.*, Prepared Statement of the FTC, *Data Security: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade*, 112th Cong. (May 4, 2011), *available at* http://www.ftc.gov/opa/2011/05/pdf/110504datasecurityhouse.pdf; Prepared Statement of the FTC, *Data Security: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade*, 112th Cong.(June 15, 2011), *available at* http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf; Prepared Statement of the FTC, *Protecting Consumers in the Modern World: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 112th Cong. (June 29, 2011), *available at* http://www.ftc.gov/os/testimony/110629privacytestimonybrill.pdf.

351 *See Comment of World Privacy Forum*, cmt. #00376, at 6; *Comment of Consumer Federation of America*, cmt. #00358, at 17-18.

consumer-facing entities could provide consumers with a link to the centralized mechanism, after having made sure that the data brokers from which they buy data participate in such a system. The Commission will discuss with relevant industry members how this mechanism could be developed and implemented voluntarily, in order to increase the transparency of their data practices and give consumers tools to opt out.[352]

b. Access to Teen Data

One commenter proposed that teens be given regular access to whether and how their data has been shared because of their particular vulnerability to ubiquitous marketing messages and heavy use of social media and mobile devices.[353] Others noted that teens in particular may not appreciate the persistence and future effects of data that they post about themselves online and thus need a "right to be forgotten." In its comment, the French Data Protection authority advocated the "right to be forgotten," which would allow consumers to withdraw data posted online about themselves at any point, for all users, but noted in particular the need to have control over information posted in one's youth.[354] In the United States, legislation has been introduced that would give teens an eraser button, which would allow them to erase certain material on social networking sites.[355]

The Commission generally supports exploration of the idea of an "eraser button," through which people can delete content that they post online. Many companies already offer this type of feature,[356] which is consistent with the principles of data access and suppression. Such an "eraser button" could be particularly useful for teens who might not appreciate the long-term consequences of their data sharing. Teens tend to be more impulsive than adults[357] and, as a result, may voluntarily disclose more information online than they should, leaving them vulnerable to identity theft or adversely affecting potential employment or college admissions opportunities. In supporting an eraser button concept, the Commission notes that such a feature

352 The current website of the Direct Marketing Association (DMA) offers an instructive model for such a mechanism. The DMA – which consists of data brokers, retailers, and others – currently offers a service through which consumers can opt out of receiving marketing solicitations via particular channels, such as direct mail, from DMA member companies. *See* DMAChoice, http://www.dmachoice.org/dma/member/home.action.

353 *See Comment of Consumers Union*, cmt. #00362, at 13; *see also Center for Digital Democracy and U.S. PIRG*, cmt. #00338, at 39.

354 *Comment of CNIL*, cmt. #00298, at 3.

355 Do Not Track Kids Act of 2011, H.R. 1895, 112th Congress (2011).

356 *See* Facebook, How Do I Remove a Wall Post or Story?, *available at* http://www.facebook.com/help/?page=174851209237562; LinkedIn, Privacy Policy, http://www.linkedin.com/static?key=privacy_policy.

357 *See, e.g.*, FTC, *Transcript of March 17, 2010, Privacy Roundtable, Panel 3: Addressing Sensitive Information*, 208-215, *available at* http://www.ftc.gov/bcp/workshops/privacyrountables/PrivacyRoundtable_March2010_Transcript.pdf; *see also* Chris Hoofnagle, Jennifer King, Su Li, & Joseph Turow, *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes & Policies?* (Apr. 14, 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864.

would have to be carefully crafted in order to avoid implicating First Amendment concerns.[358] It would also need to be technically feasible and proportional to the nature, sensitivity, and amount of data collected.

Final Principle: Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use.

3. CONSUMER EDUCATION

Proposed Principle: All stakeholders should expand their efforts to educate consumers about commercial data privacy practices.

In its preliminary report, FTC staff called for all stakeholders to accelerate their efforts to raise consumer awareness about data practices and to provide additional transparency tools to consumers. Staff pointed out that consumers need more education about the privacy implications of various data practices so that they can make informed decisions about the trade-offs involved. Staff posed questions about how the range of interested stakeholders – companies, industry associations, consumer groups, and government – can do a better job of informing consumers about privacy. Many commenters expressed general support for the notion that consumer education is a vital component of improving privacy protections for consumers.[359] One commenter suggested that businesses use their creative talents to make privacy more accessible for consumers, and as support, pointed to its own privacy game.[360] The game teaches players about privacy by inviting them to tour a virtual small town in which the buildings represent different parts of the commenter's privacy policy.

Over the last few years, a number of other companies and industry and consumer groups have stepped up their efforts to educate consumers about privacy and their privacy choices.[361] The Commission encourages more such efforts, with an eye toward developing clear and accessible messages that consumers will see and understand.

358 While consumers should be able to delete much of the information they place on a particular social media site, there may be First Amendment constraints to requiring third parties to delete the same information. In the FTC's recent proposed settlement with Facebook, the company agreed to implement measures designed to prevent any third party from accessing information under Facebook's control within a reasonable time period, not to exceed thirty days, from the time the user has deleted such information. *See In the Matter of Facebook, Inc.*, FTC File No. 092 3184 (Nov. 29, 2011) (proposed consent order), *available at* http://ftc.gov/os/caselist/0923184/111129facebookagree.pdf.

359 *See, e.g., Comment of Intuit Inc.*, cmt. #00348, at 12; *Comment of AT&T Inc.*, cmt. #00420, at 30-31; *Comment of Consumers Union*, cmt. #00362, at 18.

360 *Comment of Zynga Inc.*, cmt. #00459, at 4.

361 *See, e.g.,* Common Sense Media, App Reviews, http://www.commonsensemedia.org/app-reviews (listing reviews that evaluate privacy and safety concerns posed by common mobile applications designed for children); Google, Ad Preferences, Frequently Asked Questions, http://www.google.com/ads/preferences/html/faq.html; Interactive Advertising Bureau, Privacy Matters Campaign, http://www.iab.net/privacymatters/campaign.php; Kashmir Hill, *Zynga's PrivacyVille – It's Not Fun, But It Gets the Job Done,* FORBES, July 8, 2011, *available at* http://www.forbes.com/sites/kashmirhill/2011/07/08/zyngas-privacyville-its-not-fun-but-it-gets-the-job-done/.

A range of commenters suggested that the FTC explicitly endorse or sponsor various private sector-led consumer education efforts.[362] The Commission certainly supports private sector education efforts, and encourages private sector entities to freely use the FTC's extensive consumer and business education materials, under their own branding.

For example, the FTC encourages businesses to use information from its OnGuardOnline.gov website, which aims to help people be safe, secure and responsible online. The OnGuardOnline.gov campaign is a partnership of 15 federal agencies. The site includes articles, videos, games and tutorials to teach home users, small businesses or corporate employees about privacy-related topics like using Wi-Fi networks, peer-to-peer file sharing, mobile apps, and online tracking. The OnGuard Online Blog provides the latest cybersecurity news and practical tips from the FTC and other federal agencies. The FTC publishes this blog regularly and encourages companies to copy and disseminate it. Additionally, the FTC has continued its own consumer education efforts in the privacy area. Over the last year, the Commission released consumer education materials on a variety of topics including: using Wi-Fi hot spots; managing browser and "Flash" cookies; understanding mobile privacy; and protecting against child identity theft.[363]

Final Principle: All stakeholders should expand their efforts to educate consumers about commercial data privacy practices.

V. CONCLUSION

The final privacy framework set forth in this Report reflects the extensive record developed through the Commission's privacy roundtables as well as the over 450 public comments received in response to the proposed framework issued in December of 2010. The FTC recommends that Congress consider baseline privacy legislation while industry implements the final privacy framework through individual company initiatives and through strong and enforceable self-regulatory initiatives. As discussed throughout the report, there are a number of specific areas where policy makers have a role in assisting with the implementation of the self-regulatory principles that make up the privacy framework. Areas where the FTC will be active over the course of the next year include the following.

- **Do Not Track:** As discussed above, industry has made significant progress in implementing Do Not Track. The browser vendors have developed tools that consumers can use to signal that they do not want to be tracked; the DAA has developed its own icon-based tool and has committed to honor the browser tools; and the W3C has made substantial progress in creating an international standard for Do Not Track. However, the work is not done. The Commission will work with these groups to complete implementation of an easy-to use, persistent, and effective Do Not Track system.

362 *Comment of United States Council for International Business*, cmt. #00366, at 4; *Comment of IMS Health*, cmt. #00380, at 5; *Comment of The Privacy Projects*, cmt. #00482, at 2-3.

363 FTC, *Wise Up About Wi-Fi: Tips for Using Public Wireless Networks* (2011), http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt193.shtm; FTC, *Cookies: Leaving a Trail on the Web*, http://onguardonline.gov/articles/0042-cookies-leaving-trail-web; FTC, *Understanding Mobile Apps*, http://onguardonline.gov/articles/0018-understanding-mobile-apps; FTC Workshop, *Stolen Futures: A Forum on Child Identity Theft*, (July 12, 2011), http://www.ftc.gov/bcp/workshops/stolenfutures/.

- **Mobile:** The Commission calls on companies providing mobile services to work toward improved privacy protections, including the development of short, meaningful disclosures. To this end, FTC staff has initiated a project to update its business guidance about online advertising disclosures.[364] As part of this project, staff will host a workshop on May 30, 2012 and will address, among other issues, mobile privacy disclosures and how these disclosures can be short, effective, and accessible to consumers on small screens. The Commission hopes that the workshop will spur further industry self-regulation in this area.
- **Data Brokers:** To address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information, the Commission supports targeted legislation – similar to that contained in several of the data security bills introduced in the 112th Congress – that would provide consumers with access to information about them held by a data broker.[365] To further increase transparency, the Commission calls on data brokers that compile data for marketing purposes to explore creating a centralized website where data brokers could (1) identify themselves to consumers and describe how they collect and use consumer data and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain.
- **Large Platform Providers:** To the extent that large platforms, such as Internet Service Providers, operating systems, browsers, and social media, seek to comprehensively track consumers' online activities, it raises heightened privacy concerns. To further explore privacy and other issues related to this type of comprehensive tracking, FTC staff intends to host a public workshop in the second half of 2012.
- **Promoting enforceable self-regulatory codes:** The Department of Commerce, with the support of key industry stakeholders, is undertaking a project to facilitate the development of sector-specific codes of conduct. FTC staff will participate in that project. To the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work. The Commission will also continue to enforce the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join.

In all other areas, the Commission calls on individual companies, trade associations, and self-regulatory bodies to adopt the principles contained in the privacy framework, to the extent they have not already done so. For its part, the FTC will focus its policy efforts on the five areas identified above, vigorously enforce existing laws, work with industry on self-regulation, and continue to target its education efforts on building awareness of existing data collection and use practices and the tools to control them.

364 *See* Press Release, FTC, FTC Seeks Input to Revising its Guidance to Businesses About Disclosures in Online Advertising (May 26, 2011), *available at* http://www.ftc.gov/opa/2011/05/dotcom.shtm.

365 *See* Data Accountability and Trust Act, H.R. 1707, 112th Congress (2011); Data Accountability and Trust Act of 2011, H.R. 1841, 112th Congress (2011); Data Security and Breach Notification Act of 2011, S. 1207, 112th Congress (2011).

FTC Privacy Milestones

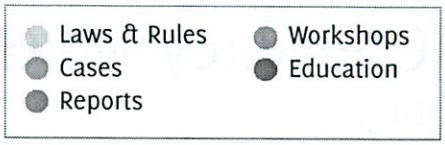
FTC Privacy Milestones

Laws & Rules · Cases · Reports · Workshops · Education

1970	Fair Credit Reporting Act enacted
1972	First Fair Credit Reporting Act (FCRA) case: In the Matter of Credit Bureau of Lorain
1975	FTC sues tax preparer for improperly using customers' information to market its loans: FTC v. Beneficial Corporation
1970s	FTC brings 15 additional enforcement actions against credit bureaus and report users
1983	First FCRA case against a nationwide credit bureau: FTC v. TransUnion
1985	FCRA sweep against users of consumer reports
1990	Commission staff issues comprehensive commentary on the FCRA
1991	FTC sues TRW for FCRA violations: FTC v. TRW
1992	FCRA sweep against employers using credit reports
1995	FTC sues Equifax for FCRA violations: In the Matter of Equifax Credit Information Services
1996	First major revision of the Fair Credit Reporting Act
	FTC sponsors workshop: *Consumer Privacy on the Global Information Infrastructure*
1997	First spam case: FTC v. Nia Cano
	FTC hosts traveling workshops to discuss revisions of FCRA
	FTC sponsors workshop: *Consumer Information Privacy*
	FTC issues *Individual Reference Services: A Federal Trade Commission Report to Congress*
1998	FTC issues *Privacy Online: A Federal Trade Commission Report to Congress*
1999	First case involving children's privacy: In the Matter of Liberty Financial
	First consumer privacy case: In the Matter of GeoCities
	FTC issues *Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress*
	FTC sponsors workshop: *Online Profiling*
	FTC launches ID Theft website: consumer.gov/idtheft and ID Theft Online Complaint Form
	FTC's 877-ID-THEFT consumer helpline established
2000	Children's Online Privacy Protection Rule (COPPA) goes into effect
	Gramm-Leach-Bliley Financial Privacy Rule goes into effect
	Three nationwide consumer reporting agencies pay $2.5 million in civil penalties for FCRA violations: US v. Equifax Credit Information Services, US v. TransUnion, and US v. Experian Information Solutions
	First COPPA case: FTC v. Toysmart.com
	FTC issues *Online Profiling: A Federal Trade Commission Report to Congress*
	FTC issues *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress*

FTC Privacy Milestones
continued

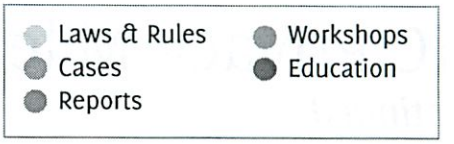
	FTC sponsors workshop: *The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*
	FTC publishes ID Theft booklet for victims: *When Bad Things Happen to Your Good Name*
2001	COPPA Safe Harbor Program begins
	First civil penalty cases under COPPA: US v. Looksmart, US v. Monarch Services, US v. Bigmailbox
	FTC sponsors workshops: *The Information Marketplace: Merging and Exchanging Consumer Data; Gramm-Leach-Bliley Educational Program on Financial Privacy;* and *Get Noticed: Effective Financial Privacy Notices: An Interagency Workshop*
	FTC publishes ID Theft Affidavit
2002	First data security case: In the Matter of Eli Lilly & Company
	FTC settles data security charges related to Microsoft's Passport service: In the Matter of Microsoft
	FTC sponsors workshop: *Consumer Information Security Workshop*
	FTC issues report on *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*
	FTC launches 10-minute educational ID Theft video
	FTC distributes over 1 million ID Theft booklets for victims
2003	Fair and Accurate Credit Transactions Act (FACTA) passed
	National Do Not Call Registry goes into effect
	Gramm-Leach-Bliley Safeguards Rule goes into effect
	FTC sues companies for sharing students' survey data with commercial marketers: In the Matter of Education Research Center of America and Student Marketing Group
	Guess settles FTC data security charges: In the Matter of Guess?
	FTC issues *Technologies for Protecting Personal Information: A Staff Workshop Report*
	FTC sponsors workshops: *Technologies for Protecting Personal Information; Spam Forum;* and *Costs and Benefits Related To the Collection and Use of Consumer Information*
2004	CAN-SPAM Rule goes into effect
	CAN-SPAM Adult Labeling Rule goes into effect
	Free Annual Credit Report Rule goes into effect
	First spyware case: FTC v. Seismic Entertainment
	FTC charges company with exposing consumers' purchases: In the Matter of MTS (dba Tower Records)
	FTC charges company with renting consumer information it had pledged to keep private: In the Matter of Gateway Learning



	FTC issues *The CAN-SPAM Act of 2003: National Do Not Email Registry: A Federal Trade Commission Report to Congress*
	FTC sponsors workshops: *Monitoring Software on Your PC: Spyware, Adware and Other Software; Radio Frequency IDentification: Applications and Implications for Consumers;* and *Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues*
	FTC publishes *The CAN-SPAM Act: A Compliance Guide for Business*
2005	FACTA Disposal Rule goes into effect
	FACTA Pre-Screen Opt Out Rule goes into effect
	National Do Not Call Registry tops 100 million phone numbers
	First Do Not Call enforcement action: FTC v. National Consumer Council
	First Do Not Call civil penalty action: US v. Braglia Marketing
	Highest civil penalty in a Do Not Call case: US v. DirecTV ($5.3 million)
	First enforcement actions under Gramm-Leach-Bliley Safeguards Rule: In the Matter of Sunbelt Lending and In the Matter of Nationwide Mortgage Group
	First unfairness allegation in a data security case: In the Matter of BJ's Wholesale Club
	FTC issues *RFID: Radio Frequency IDentification: Applications and Implications for Consumers: A Workshop Report From the Staff of the Federal Trade Commission*
	FTC issues *Spyware Workshop: Monitoring Software On Your Personal Computer: Spyware, Adware, and Other Software: Report of the Federal Trade Commission Staff*
	FTC launches online safety website: OnGuardOnline.gov
2006	FACTA Rule Limiting Marketing Solicitations from Affiliates goes into effect
	Highest civil penalty in a consumer protection case: US v. ChoicePoint ($10 million civil penalty for violations of FCRA as well as $5 million redress for victims)
	First adware case: In the Matter of Zango
	Highest civil penalty to date in a COPPA case: US v. Xanga ($1 million)
	FTC settles charges against a payment processor that had experienced the largest breach of financial data to date: In the Matter of CardSystems Solutions
	FTC issues *Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues: A Federal Trade Commission Staff Workshop Report*
	FTC sponsors workshop: *Protecting Consumers in the Next Tech-Ade*
	FTC launches national educational campaign on identity theft and publishes *Deter, Detect, Defend: Avoid ID Theft* brochure

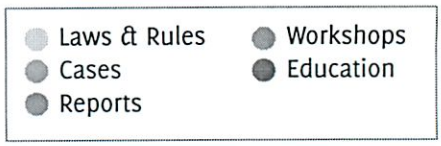
FTC Privacy Milestones
continued

2007	First Disposal Rule case: US v. American United Mortgage Company
	Adult-oriented online social networking operation settles FTC charges; unwitting consumers pelted with sexually graphic pop-ups: FTC v. Various (dba AdultFriendFinder)
	FTC issues *Spam Summit: The Next Generation of Threats and Solutions: A Staff Report by the Federal Trade Commission's Division of Marketing Practices*
	FTC issues *Implementing the Children's Online Privacy Protection Act: A Federal Trade Commission Report to Congress*
	FTC co-chairs President's Identity Theft Task Force (with DOJ) and issues Strategic Plan
	FTC sponsors workshops: *Security in Numbers: SSNs and ID Theft; Ehavioral Advertising: Tracking, Targeting, and Technology*; and *Spam Summit: The Next Generation of Threats and Solutions*
	FTC publishes *Protecting Personal Information: A Guide for Business* and launches interactive tutorial
2008	Highest civil penalty in a CAN-SPAM case: US v. ValueClick ($2.9 million)
	FTC settles charges against data broker Lexis Nexis and retailer TJX related to the compromise of hundreds of thousands of consumers' information: In the Matter of Reed Elsevier and Seisent and In the Matter of TJX Companies
	FTC issues *Protecting Consumers in the Next Tech-ade: A Report by the Staff of the Federal Trade Commission*
	FTC issues *Security In Numbers: Social Security Numbers and Identity Theft – A Federal Trade Commission Report Providing Recommendations On Social Security Number Use In the Private Sector*
	President's Identity Theft Task Force Report released
	FTC sponsors workshops: *Protecting Personal Information: Best Practices for Business* (Chicago, Dallas, and Los Angeles); *Pay on the Go: Consumers and Contactless Payment, Transatlantic RFID Workshop on Consumer Privacy and Data Security*; and *Beyond Voice: Mapping the Mobile Marketplace*
	U.S. Postal Service sends FTC ID Theft prevention brochure to every household in the country
2009	Robocall Rule goes into effect
	Health Breach Notification Rule goes into effect
	First case alleging failure to protect employee information: In the Matter of CVS Caremark
	First cases alleging six companies violated the EU-US Safe Harbor Agreement: In the Matter of World Innovators, In the Matter of ExpatEdge Partners, In the Matter of Onyx Graphics, In the Matter of Directors Desk, In the Matter of Progressive Gaitways, and In the Matter of Collectify
	FTC issues *Self-Regulatory Principles For Online Behavioral Advertising: Tracking, Targeting, and Technology*



	FTC sponsors workshops: *Exploring Privacy: A Roundtable Series*; *Protecting Personal Information: Best Practices for Business* (New York); and *Securing Personal Data in the Global Economy*
	FTC publishes *Net Cetera: Chatting with Kids About Being Online*
2010	FTC jointly publishes Model Privacy Form under the Gramm-Leach-Bliley Act
	National Do Not Call Registry tops 200 million phone numbers
	First data security case involving social media: In the Matter of Twitter
	First case shutting down a rogue ISP: FTC v. Pricewert
	First data security case against an online seal provider: FTC v. ControlScan
	Highest judgment in a spyware case: FTC v. Innovative Marketing ($163 million)
	Largest FTC-state coordinated settlement on privacy: FTC v. Lifelock
	FTC conducts sweep against companies for exposure of employee and/or customer data on peer-to-peer (P2P) file-sharing networks
	FTC releases Preliminary FTC Staff Report *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*
	FTC sponsors *COPPA Rule Review Roundtable*
	FTC publishes *Peer-to-Peer File Sharing: A Guide for Businesses*; *Medical Identity Theft: How to Minimize Your Risk*; and *Copier Data Security: A Guide for Businesses*
	FTC distributes 6+ million printed copies of *Deter, Detect, Defend: Avoid ID Theft* brochures and 5+ million printed copies of *Net Cetera: Chatting with Kids About Being Online*
2011	FTC seeks comment on proposed changes to COPPA rule
	First case alleging substantive Safe Harbor violation and imposing privacy assessment program and audit requirements: In the Matter of Google
	First case against an online advertising network for offering deceptive privacy controls: In the Matter of Chitika
	First COPPA case against a mobile application developer: US v. W3 Innovations
	First case alleging unfairness based on default privacy settings: FTC v. Frostwire
	Largest FTC privacy case to date: In the Matter of Facebook
	FTC releases report *40 Years of Experience with the Fair Credit Reporting Act*
	FTC co-hosts *Stolen Futures: A Forum on Child ID Theft*
	FTC hosts *Face Facts: A Forum on Facial Recognition* Workshop
	FTC publishes *Tips for Using Public Wireless Networks*
	FTC publishes *Facts from the FTC: What You Should Know About Mobile Apps*
	FTC publishes *Online Safety for Teens and Tweens*

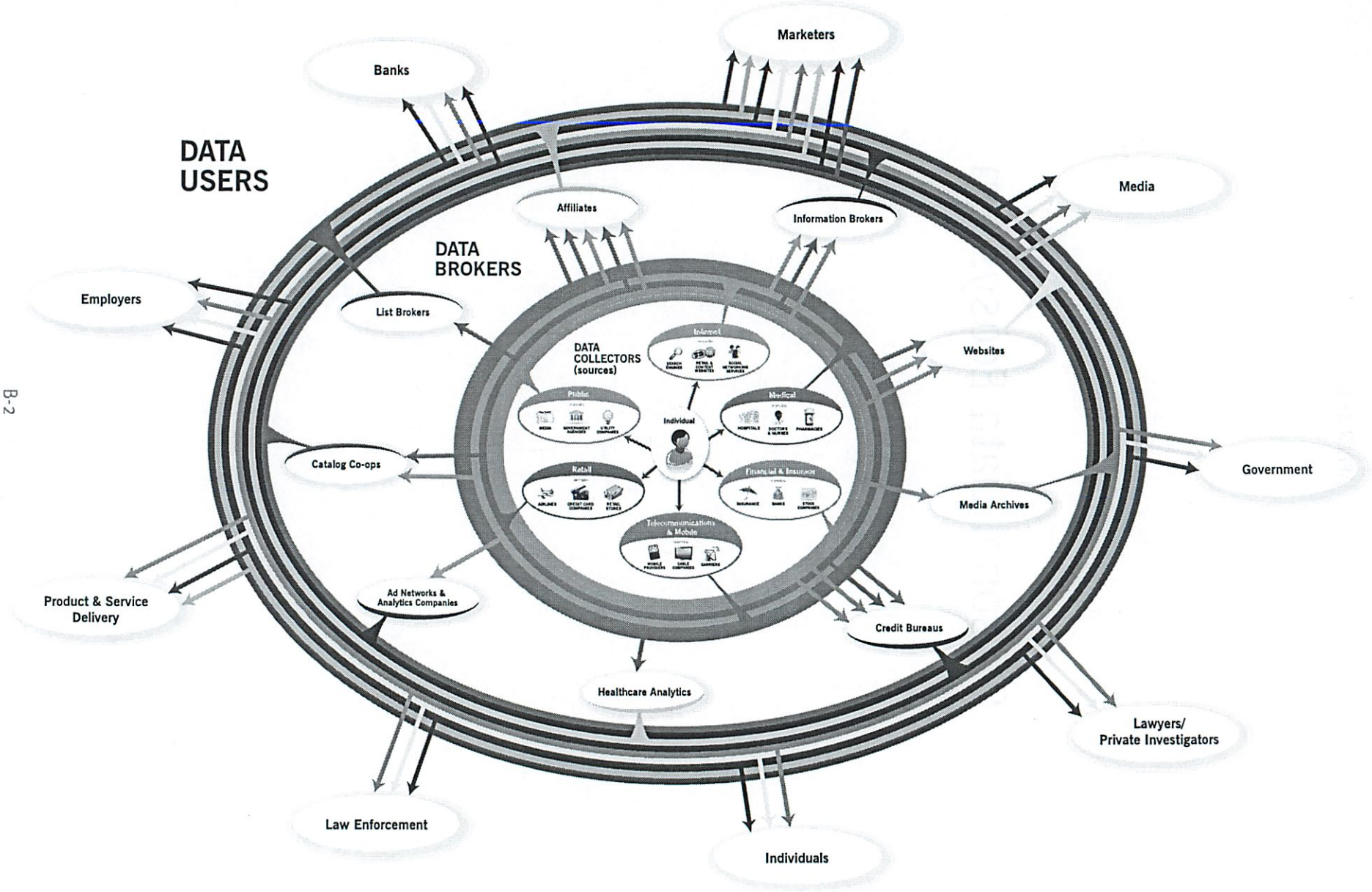
FTC Privacy Milestones
continued



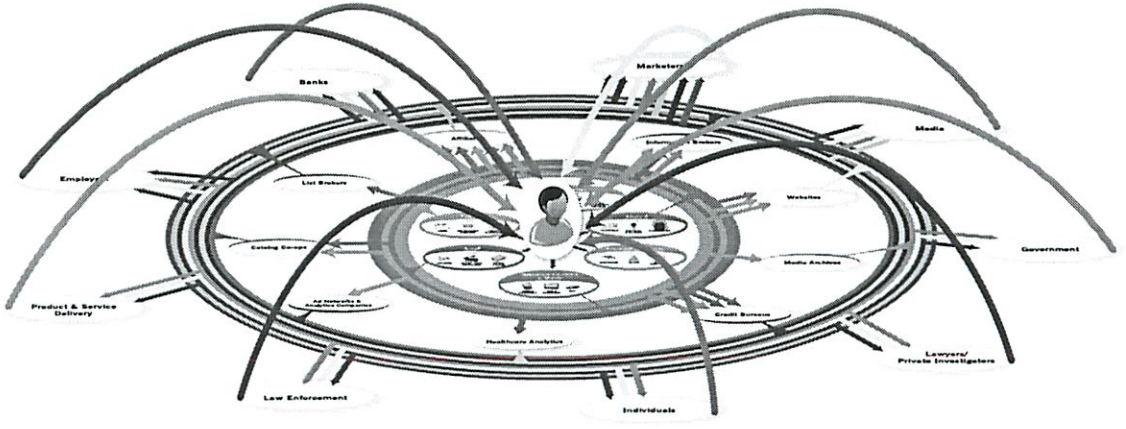
2012	FTC releases report *Using FACTA Remedies: An FTC Staff Report on a Survey of Identity Theft Victims*
	FTC releases report *Mobile Apps for Kids: Current Privacy Disclosures Are Disappointing*
	FTC announces workshop: *Paper, Plastic... or Mobile? An FTC Workshop on Mobile Payments*
	FTC announces workshop to Explore Disclosures in Online and Mobile Media
	FTC publishes Blog Post: *FCRA & Mobile Apps: A Word of Warning*

Personal Data Ecosystem

Personal Data Ecosystem



DATA USES:



Examples of uses of consumer information in personally identifiable or aggregated form:

- Financial services, such as for banking or investment accounts
- Credit granting, such as for credit or debit cards; mortgage, automobile or specialty loans; automobile rentals; or telephone services
- Insurance granting, such as for health, automobile or life
- Retail coupons and special offers
- Catalog and magazine solicitations
- Web and mobile services, including content, e-mail, search, and social networking
- Product and service delivery, such as streaming video, package delivery, or a cable signal
- Attorneys, such as for case investigations
- Journalism, such as for fact checking
- Marketing, whether electronically, through direct mail, or by telephone
- Data brokers for aggregation and resale to companies and/or consumers
- Background investigations by employers or landlords
- Locating missing or lost persons, beneficiaries, or witnesses
- Law enforcement
- Research (e.g., health, financial, and online search data) by academic institutions, government agencies, and commercial companies
- Fraud detection and prevention
- Government benefits and services, such as licensing

Dissenting Statement of Commissioner J. Thomas Rosch

tracking. But, as I have said, consumer surveys are inconclusive, and individual consumers by and large do not "opt out" from tracking when given the chance to do so.[6] Not surprisingly, large enterprises in highly concentrated industries, which may be tempted to raise the privacy bar so high that it will disadvantage rivals, also support adopting more stringent privacy principles.[7]

The "final" Privacy Report (incorporating the preliminary staff report) repeatedly sides with consumer organizations and large enterprises. It proceeds on the premise that behavioral tracking is "unfair."[8] Thus, the Report expressly recommends that "reputational harm" be considered a type of harm that the Commission should redress.[9] The Report also expressly says that privacy be the default setting for commercial data practices.[10] Indeed, the Report says that the "traditional distinction between PII and non-PII has blurred,"[11] and it recommends "shifting the burdens away from consumers and placing obligations on businesses."[12] To the extent the Report seeks consistency with international privacy standards,[13] I would urge caution. We should always carefully consider whether each individual policy choice regarding privacy is appropriate for this country in all contexts.

That is not how the Commission itself has traditionally proceeded. To the contrary, the Commission represented in its 1980, and 1982, Statements to Congress that, absent deception, it will not generally enforce Section 5 against alleged intangible harm.[14] In other contexts, the Commission has tried, through its advocacy, to convince others that our policy judgments are sensible and ought to be adopted. And, as I stated in connection with the recent *Intel* complaint, in the competition context, one of the principal virtues

---

6 *See* Katy Bachman, *Study: Internet User Adoption of DNT Hard to Predict*, adweek.com, March 20, 2012, *available at* http://www.adweek.com/news/technology/study-internet-user-adoption-dnt-hard-predict-139091 (reporting on a survey that found that what Internet users say they are going to do about using a Do Not Track button and what they are currently doing about blocking tracking on the Internet, are two different things); *see also* Concurring Statement of Commissioner J. Thomas Rosch, Issuance of Preliminary FTC Staff Report "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" (Dec. 1, 2010), *available at* http://www.ftc.gov/speeches/rosch/101201privacyreport.pdf.

7 *See* J. Thomas Rosch, Comm'r, Fed. Trade Comm'n, Do Not Track: Privacy in an Internet Age, Remarks at Loyola Chicago Antitrust Institute Forum, (Oct. 14, 2011), *available at* http://www.ftc.gov/speeches/rosch/111014-dnt-loyola.pdf; *see also* Report at 9.

8 Report at 8 and n.37.

9 *Id.* at 2. The Report seems to imply that the Do Not Call Rule would support this extension of the definition of harm. *See id.* ("unwarranted intrusions into their daily lives"). However, it must be emphasized that the *Congress* granted the FTC underlying authority under the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101-6108, to promulgate the Do Not Call provisions and other substantial amendments to the TSR. The Commission did not do so unilaterally.

10 *Id.*

11 *Id.* at 19.

12 *Id.* at 23, *see also id.* at 24.

13 *Id.* at 9-10. This does not mean that I am an isolationist or am impervious to the benefits of a global solution. But, as stated below, there is more than one way to skin this cat.

14 *See* Letter from the FTC to Hon. Wendell Ford and Hon. John Danforth, Committee on Commerce, Science and Transportation, United States Senate, Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980), reprinted in International Harvester Co., 104 F.T.C. 949, 1070, 1073 (1984) ("Unfairness Policy Statement") *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm; Letter from the FTC to Hon. Bob Packwood and Hon. Bob Kasten, Committee on Commerce, Science and Transportation, United States Senate, reprinted in FTC Antitrust & Trade Reg. Rep. (BNA) 1055, at 568-570 ("Packwood-Kasten letter"); and 15 U.S.C. § 45(n), which codified the FTC's modern approach.

Dissenting Statement of Commissioner J. Thomas Rosch
Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers
March 26, 2012

Introduction

I agree in several respects with what the "final" Privacy Report says. Specifically, although I disagree that the consumer has traditionally ever been given any "choice" about information collection practices (other than to "take-it-or-leave-it" after reviewing a firm's privacy notice), I agree that consumers ought to be given a broader range of choices if for no other reason than to customize their privacy protection. However, I still worry about the constitutionality of banning take-it-or-leave-it choice (in circumstances where the consumer has few alternatives); as a practical matter, that prohibition may chill information collection, and thus impact innovation, regardless whether one's privacy policy is deceptive or not.[1]

I also applaud the Report's recommendation that Congress enact "targeted" legislation giving consumers "access" to correct misinformation about them held by a data broker.[2] I also support the Report's recommendation that Congress implement federal legislation that would require entities to maintain reasonable security and to notify consumers in the event of certain security breaches.[3]

Finally, I concur with the Report insofar as it recommends that information brokers who compile data for marketing purposes must disclose to consumers how they collect and use consumer data.[4] I have long felt that we had no business counseling Congress or other agencies about privacy concerns without that information. Although I have suggested that compulsory process be used to obtain such information (because I am convinced that is the only way to ensure that our information is complete and accurate),[5] a voluntary centralized website is arguably a step in the right direction.

Privacy Framework

My disagreement with the "final" Privacy Report is fourfold. First, the Report is rooted in its insistence that the "unfair" prong, rather than the "deceptive" prong, of the Commission's Section 5 consumer protection statute, should govern information gathering practices (including "tracking"). "Unfairness" is an elastic and elusive concept. What is "unfair" is in the eye of the beholder. For example, most consumer advocacy groups consider behavioral tracking to be unfair, whether or not the information being tracked is personally identifiable ("PII") and regardless of the circumstances under which an entity does the

1 *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* ("Report") at 50-52.

2 *Id.* at 14, 73.

3 *Id.* at 26. I also support the recommendation that such legislation authorize the Commission to seek civil penalties for violations. However, despite its bow to "targeted" legislation, the Report elsewhere counsels that the Commission support privacy legislation generally. *See, e.g., id.* at 16. To the extent that those recommendations are not defined, or narrowly targeted, I disagree with them.

4 *Id.* at 14, 68-70.

5 *See* J. Thomas Rosch, Comm'r, Fed. Trade Comm'n, Information and Privacy: In Search of a Data-Driven Policy, Remarks at the Technology Policy Institute Aspen Forum (Aug. 22, 2011), *available at* http://www.ftc.gov/speeches/rosch/110822aspeninfospeech.pdf.

of applying Section 5 was that that provision was "self-limiting," and I advocated that Section 5 be applied on a stand-alone basis only to a firm with monopoly or near-monopoly power.[15] Indeed, as I have remarked, absent such a limiting principle, privacy may be used as a weapon by firms having monopoly or near-monopoly power.[16]

There does not appear to be any such limiting principle applicable to many of the recommendations of the Report. If implemented as written, many of the Report's recommendations would instead apply to almost all firms and to most information collection practices. It would install "Big Brother" as the watchdog over these practices not only in the online world but in the offline world.[17] That is not only paternalistic, but it goes well beyond what the Commission said in the early 1980s that it would do, and well beyond what Congress has permitted the Commission to do under Section 5(n).[18] I would instead stand by what we have said and challenge information collection practices, including behavioral tracking, only when these practices are deceptive, "unfair" within the strictures of Section 5(n) and our commitments to Congress, or employed by a firm with market power and therefore challengeable on a stand-alone basis under Section 5's prohibition of unfair methods of competition.

Second, the current self-regulation and browser mechanisms for implementing Do Not Track solutions may have advanced since the issuance of the preliminary staff Report.[19] But, as the final Report concedes, they are far from perfect,[20] and they may never be, despite efforts to create a standard through the World Wide Web Consortium ("W3C") for the browser mechanism.[21]

More specifically, as I have said before, the major browser firms' interest in developing Do Not Track mechanisms begs the question of whether and to what extent those major browser firms will act strategically and opportunistically (to use privacy to protect their own entrenched interests).[22]

In addition, the recent announcement by the Digital Advertising Alliance (DAA) that it will honor the tracking choices consumers make through their browsers raises more questions than answers for me. The Report is not clear, and I am concerned, about the extent to which this latest initiative will displace the standard-setting effort that has recently been undertaken by the W3C. Furthermore, it is not clear that all the interested players in the Do Not Track arena – whether it be the DAA, the browser firms, the W3C, or consumer advocacy groups – will be able to come to agreement about what "Do Not Track" even means.[23] It may be that the firms professing an interest in self-regulation are really talking about a "Do Not Target" mechanism, which would only prevent a firm from serving targeted ads, rather than a "Do Not Track"

15 *See* Concurring and Dissenting Statement of Commissioner J. Thomas Rosch, *In re Intel Corp.*, Docket No. 9341, (Dec. 16, 2009), *available at* http://www.ftc.gov/os/adjpro/d9341/091216intelstatement.pdf.

16 *See* Rosch, *supra* note 7 at 20.

17 *See* Report at 13.

18 Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-312.

19 Report at 4, 52.

20 *Id.* at 53, 54; *see esp. id.* at 53 n.250.

21 *Id.* at 5, 54.

22 *See* Rosch, *supra* note 7 at 20-21.

23 Tony Romm, "*What Exactly Does 'Do Not Track' Mean?*," Politico, Mar. 13, 2012, *available at* http://www.politico.com/news/stories/0312/73976.html; *see also* Report at 4 (DAA allows consumer to opt out of "targeted advertising").

mechanism, which would prevent the collection of consumer data altogether. For example, the DAA's Self-Regulatory Principles for Multi-Site Data do not apply to data collected for "market research" or "product development."[24] For their part, the major consumer advocacy groups may not be interested in a true "Do Not Track" mechanism either. They may only be interested in a mechanism that prevents data brokers from compiling consumer profiles instead of a comprehensive solution. It is hard to see how the W3C can adopt a standard unless and until there is an agreement about what the standard is supposed to prevent.[25]

It is also not clear whether or to what extent the lessons of the Carnegie Mellon Study respecting the lack of consumer understanding of how to access and use Do Not Track will be heeded.[26] Similarly, it is not clear whether and to what extent Commissioner Brill's concern that consumers' choices, whether it be "Do Not Collect" or merely "Do Not Target," will be honored.[27] Along the same lines, it is also not clear whether and to what extent a "partial" Do Not Track solution (offering nuanced choice) will be offered or whether it is "all or nothing." Indeed, it is not clear whether consumers can or will be given complete and accurate information about the pros and the cons of subscribing to Do Not Track before they choose it. I find this last question especially vexing in light of a recent study that indicated 84% of users polled prefer targeted advertising in exchange for free online content.[28]

Third, I am concerned that "opt-in" will necessarily be selected as the *de facto* method of consumer choice for a wide swath of entities that have a first-party relationship with consumers but who can potentially track consumers' activities across unrelated websites, under circumstances where it is unlikely, because of the "context" (which is undefined) for such tracking to be "consistent" (which is undefined) with that first-party relationship:[29] 1) companies with multiple lines of business that allow data collection in different contexts (such as Google);[30] 2) "social networks," (such as Facebook and Twitter), which could potentially use "cookies," "plug-ins," applications, or other mechanisms to track a consumer's activities across

---

24 *See Self-Regulatory Principles for Multi-Site Data,* Digital Advertising Alliance, Nov. 2011, at 3, 10, 11, *available at* http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf; *see also* Tanzina Vega, *Opt-Out Provision Would Halt Some, but Not All, Web Tracking*, New York Times, Feb. 26, 2012, *available at* http://www.nytimes.com/2012/02/27/technology/opt-out-provision-would-halt-some-but-not-all-web-tracking.html?pagewanted=all.

25 *See* Vega, *supra* note 24.

26 *"Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising,"* Carnegie Mellon University CyLab, Oct. 31, 2011, *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11017.pdf; *see also Search Engine Use 2012,* at 25, Pew Internet & American Life Project, Pew Research Center, Mar. 9, 2012, *available at* http://pewinternet.org/~/media/Files/Reports/2012/PIP_Search_Engine_Use_2012.pdf ("[j]ust 38% of internet users say they are generally aware of ways they themselves can limit how much information about them is collected by a website").

27 *See* Julie Brill, Comm'r, Fed. Trade Comm'n, Big Data, Big Issues, Remarks at Fordham University School of Law (Mar. 2, 2012) *available at* http://www.ftc.gov/speeches/brill/120228fordhamlawschool.pdf.

28 *See* Bachman, *supra* note 6.

29 Report at 41.

30 *Id.* Notwithstanding that Google's prospective conduct seems to fit perfectly the circumstances set forth on this page of the Report (describing a company with multiple lines of business including a search engine and ad network), where the Commission states "consumer choice" is warranted, the Report goes on to conclude on page 56 that Google's practices do not require affirmative express consent because they "currently are not so widespread that they could track a consumer's every movement across the Internet."

the Internet;[31] and 3) "retargeters," (such as Amazon or Pacers), which include a retailer who delivers an ad on a third-party website based on the consumer's previous activity on the retailer's website.[32]

These entities might have to give consumers "opt-in" choice now or in the future: 1) regardless whether the entity's privacy policy and notices adequately describe the information collection practices at issue; 2) regardless of the sensitivity of the information being collected; 3) regardless whether the consumer cares whether "tracking" is actually occurring; 4) regardless of the entity's market position (whether the entity can use privacy strategically – *i.e.*, an opt-in requirement – in order to cripple or eliminate a rival); and 5) conversely, regardless whether the entity can compete effectively or innovate, as a practical matter, if it must offer "opt in" choice.[33]

Fourth, I question the Report's apparent mandate that ISPs, with respect to uses of deep packet inspection, be required to use opt-in choice.[34] This is not to say there is no basis for requiring ISPs to use opt-in choice without requiring opt-in choice for other large platform providers. But that kind of "discrimination" cannot be justified, as the Report says, because ISPs have "are in a position to develop highly detailed and comprehensive profiles of their customers."[35] So does any large platform provider who makes available a browser or operating system to consumers.[36]

Nor can that "discrimination" be justified on the ground that ISPs may potentially use that data to "track" customer behavior in a fashion that is contrary to consumer expectations. There is no reliable data establishing that most ISPs presently do so. Indeed, with a business model based on subscription revenue, ISPs arguably lack the same incentives as do other platform providers whose business model is based on attracting advertising and advertising revenue: ISPs assert that they track data only to perform operational and security functions; whereas other platform providers that have business models based on advertising revenue track data in order to maximize their advertising revenue.

What really distinguishes ISPs from most other "large platform providers" is that their markets can be highly concentrated.[37] Moreover, even when an ISP operates in a less concentrated market, switching costs can be, or can be perceived as being, high.[38] As I said in connection with the *Intel* complaint, a monopolist or near monopolist may have obligations which others do not have.[39] The only similarly situated platform provider may be Google, which, because of its alleged monopoly power in the search advertising market,

31 *Id.* at 40. *See also supra* note 30. That observation also applies to "social networks" like Facebook.

32 *Id.* at 41.

33 *See id.* at 60 ("Final Principle").

34 *Id.* at 56 ("the Commission has strong concerns about the use of DPI for purposes inconsistent with an ISP's interaction with a consumer, without express affirmative consent or more robust protection").

35 *Id.*

36 *Id.*

37 Federal Communications Commission, *Connecting America: The National Broadband Plan, Broadband Competition and Innovation Policy, Section 4.1, Networks, Competition in Residential Broadband Markets* at 36, *available at* http://www.broadband.gov/plan/4-broadband-competition-and-innovation-policy/.

38 Federal Communications Commission Working Paper, *Broadband decisions: What drives consumers to switch – or stick with – their broadband Internet provider* (Dec. 2010), at 3, 8, *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2010/db1206/DOC-303264A1.pdf.

39 *See* Rosch, *supra* note 15.

has similar power. For any of these "large platform providers," however, affirmative express consent should be required only when the provider *actually* wants to use the data in this fashion, not just when it *has the potential* to do so.[40]

Conclusion

Although the Chairman testified recently before the House Appropriations Subcommittee chaired by Congresswoman Emerson that the recommendations of the final Report are supposed to be nothing more than "best practices,"[41] I am concerned that the language of the Report indicates otherwise, and broadly hints at the prospect of enforcement.[42] The Report also acknowledges that it is intended to serve as a template for legislative recommendations.[43] Moreover, to the extent that the Report's "best practices" mirror the Administration's privacy "Bill of Rights," the President has specifically asked either that the "Bill of Rights" be adopted by the Congress or that they be distilled into "enforceable codes of conduct."[44] As I testified before the same subcommittee, this is a "tautology;" either these practices are to be adopted voluntarily by the firms involved or else there is a federal requirement that they be adopted, in which case there can be no pretense that they are "voluntary."[45] It makes no difference whether the federal requirement is in the form of enforceable codes of conduct or in the form of an act of Congress. Indeed, it is arguable that neither is needed if these firms feel obliged to comply with the "best practices" or face the wrath of "the Commission" or its staff.

---

40 *See, e.g.*, Report at 56.

41 Testimony of Jon Leibowitz and J. Thomas Rosch, Chairman and Comm'r, FTC, *The FTC in FY2013: Protecting Consumers and Competition: Hearing on Budget Before the H. Comm. on Appropriations Subcomm. on Financial Services and General Government*, 112th Cong. 2 (2012), text from CQ Roll Call, available from: LexisNexis® Congressional.

42 One notable example is found where the Report discusses the articulation of privacy harms and enforcement actions brought on the basis of *deception*. The Report then notes "[l]ike these enforcement actions, a privacy framework should address practices that unexpectedly reveal previously private information even absent physical or financial harm, or unwarranted intrusions." Report at 8. The accompanying footnote concludes that "even in the absence of such misrepresentations, revealing previously-private consumer data could cause consumer harm." *See also infra* note 43.

43 *Id.* at 16 ("to the extent Congress enacts any of the Commission's recommendations through legislation"); *see also id.* at 12-13 ("the Commission calls on Congress to develop baseline privacy legislation that is technologically neutral and sufficiently flexible to allow companies to continue to innovate").

44 *See* Letter from President Barack Obama, *appended to* White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 23, 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

45 *See* FTC Testimony, *supra* note 41.

FEDERAL TRADE COMMISSION | FTC.GOV

I did
I actually
download

Privacy on the Books and on the Ground

Kenneth A. Bamberger
University of California, Berkeley - School of Law

Deirdre K. Mulligan
University of California, Berkeley - School of Information

November 18, 2011

Stanford Law Review, Vol. 63, January 2011
UC Berkeley Public Law Research Paper No. 1568385

Abstract:
U.S. privacy law is under attack. Scholars and advocates criticize it as weak, incomplete, and confusing, and argue that it fails to empower individuals to control the use of their personal information. These critiques present a largely accurate description of the law "on the books." But the debate has strangely ignored privacy "on the ground" - since 1994, no one has conducted a sustained inquiry into how corporations actually manage privacy, and what motivates them.

This Article presents findings from the first study of corporate privacy management in fifteen years, involving qualitative interviews with Chief Privacy Officers identified by their peers as industry leaders. Spurred by these findings, we present a descriptive account of privacy "on the ground" that upends the terms of the prevailing policy debate. This alternative account identifies elements neglected by the traditional story - the emergence of the Federal Trade Commission as a privacy regulator, the increasing influence of privacy advocates, market and media pressures for privacy-protection, and the rise of privacy professionals - and traces the ways in which these players supplemented a privacy debate largely focused on processes (such as notice and consent mechanisms) with a growing emphasis on substance: preventing violations of consumers' expectations of privacy.

This "grounded" account should inform privacy reforms. While widespread efforts to expand consent mechanisms to empower individuals to control their personal information may offer some promise, those efforts should not proceed in a way that eclipses robust substantive definitions of privacy and the protections they are beginning to produce, or that constrains the regulatory flexibility that permits their evolution. This would destroy important tools for limiting corporate over-reaching, curbing consumer manipulation, and protecting shared expectations about the personal sphere on the Internet, and in the marketplace.

Number of Pages in PDF File: 70

Keywords: privacy, regulation, consumer protection, chief privacy officers, Federal Trade

I think I did
(looks like no

Commission, data protection, new governance, organizational fields, professionalization

JEL Classification: D73, D81, K20, K23, O38

Accepted Paper Series

Date posted: March 11, 2010 ; **Last revised:** November 23, 2011

Download This Paper

Suggested Citation

Bamberger, Kenneth A. and Mulligan, Deirdre K., Privacy on the Books and on the Ground (November 18, 2011). Stanford Law Review, Vol. 63, January 2011; UC Berkeley Public Law Research Paper No. 1568385. Available at SSRN: http://ssrn.com/abstract=1568385

Contact Information

Kenneth A. Bamberger (Contact Author)

University of California, Berkeley - School of Law (email)
Boalt Hall
Berkeley, CA 94720-7200
United States
(510) 643-6218 (Phone)
HOME PAGE: http://www.law.berkeley.edu/faculty/profiles/facultyProfile.php?facID=5701

Deirdre K. Mulligan

University of California, Berkeley - School of Information
(email)
102 South Hall
Berkeley, CA 94720-4600
United States

Technology Liberation Front

Keeping politicians' hands off the Net & everything else related to technology

- Home
- About Us
- Archives
- Ongoing Series
- Tech Policy Events
- Podcast
- Subscribe

White House Ignores Real Bill of Rights in Call for Privacy Regulation of Internet Businesses

by Berin Szoka on February 23, 2012 · Add a Comment

The White House's "Consumer Data Privacy in a Networked World" report outlines a revised framework for consumer privacy, proposes a "Consumer Privacy Bill of Rights," and calls on Congress to pass new legislation to regulate online businesses. The following statement can be attributed to Berin Szoka, President of TechFreedom, and Larry Downes, TechFreedom Senior Adjunct Fellow:

> This Report begins and ends as constitutional sleight-of-hand. President Obama starts by reminding us of the Fourth Amendment's essential protection against "unlawful intrusion into our homes and our personal papers"—by government. But the Report recommends no reform whatsoever for outdated laws that have facilitated a dangerous expansion of electronic surveillance. That is the true threat to our privacy. The report dismisses it in a footnote.
>
> Instead, the Report calls for extensive new regulation of Internet businesses to address little more than the growing pains of a vibrant emerging economy. "For businesses to succeed online," President Obama asserts, "consumers must feel secure." Yet online businesses that rely on data to deliver innovative and generally free services are the one bright spot in a sour economy. Experience has shown consumers ultimately bear the costs of regulations imposed on emerging technologies, no matter how well-intentioned.
>
> The report is a missed opportunity. The Administration should have called for increased protections against government's privacy intrusions. Focusing on the real Bill of Rights would have respected not only the Fourth Amendment, but also the First Amendment. The Supreme Court made clear last year that the private sector's use of data is protected speech—an issue also not addressed by this Report.

Szoka and Downes are available for comment at media@techfreedom.org.

THE CASE FOR THE THIRD-PARTY DOCTRINE

*Orin S. Kerr**

This Article offers a defense of the Fourth Amendment's third-party doctrine, the controversial rule that information loses Fourth Amendment protection when it is knowingly revealed to a third party. Fourth Amendment scholars have repeatedly attacked the rule on the ground that it is unpersuasive on its face and gives the government too much power. This Article responds that critics have overlooked the benefits of the rule and have overstated its weaknesses.

The third-party doctrine serves two critical functions. First, the doctrine ensures the technological neutrality of the Fourth Amendment. It corrects for the substitution effect of third parties that would otherwise allow savvy criminals to substitute a hidden third-party exchange for a previously public act. Second, the doctrine helps ensure the clarity of Fourth Amendment rules. It matches the Fourth Amendment rules for information to the rules for location, creating clarity without the need for a complex framework of sui generis rules.

Finally, the two primary criticisms of the third-party doctrine are significantly weaker than critics have claimed. The third-party doctrine is awkward for reasons of form rather than function; it is a consent rule disguised as an application of Katz*'s "reasonable expectation of privacy" test. Claims that the doctrine gives the government too much power overlook the substitutes for Fourth Amendment protection in the use of the third parties. Those substitutes include entrapment law, common law privileges, the* Massiah *doctrine, the First Amendment, internal agency regulations, and the rights of the third parties themselves.*

---

* Professor, George Washington University Law School. This Article benefited greatly from thoughtful comments during workshops at Seton Hall, Widener-Wilmington, and the GW/Berkeley Privacy Law Scholars Conference. Thanks in particular to Daniel Solove, Christopher Slobogin, David Feige, Stephen Henderson, and Christine Jolls.

TABLE OF CONTENTS

INTRODUCTION

Human beings are social animals. We like to share. We like to gossip. We ask for help from others, and we give help in return. Sometimes we share by speaking in person. Sometimes we write a letter or send a message by computer. In all of these cases, the human impulse to share creates an important opportunity for criminal investigators. When wrongdoers share with others, they often expose evidence of their crimes. A corrupt

businessman might disclose records to his accountant. A mob boss might tell his brother about an assault. A drug dealer might reveal his plans to a confidential informant. In all of these cases, someone other than the criminal or the police—some third party—comes to possess evidence of crime. Investigators often want to collect evidence from these third parties, as they are more likely to cooperate and less likely to tip off the suspect that an investigation is afoot.

The "third-party doctrine" is the Fourth Amendment rule that governs collection of evidence from third parties in criminal investigations.[1] The rule is simple: By disclosing to a third party, the subject gives up all of his Fourth Amendment rights in the information revealed. According to the Supreme Court:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[2]

In other words, a person cannot have a reasonable expectation of privacy in information disclosed to a third party.[3] The Fourth Amendment simply does not apply.

The third-party doctrine is the Fourth Amendment rule scholars love to hate. It is the *Lochner*[4] of search and seizure law, widely criticized as profoundly misguided.[5] Decisions applying the doctrine "top[] the chart of [the]

---

1. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 528–29 (2006) (describing the third-party doctrine).

2. United States v. Miller, 425 U.S. 435, 443 (1976).

3. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

4. Lochner v. New York, 198 U.S. 45 (1905).

5. A list of every article or book that has criticized the doctrine would make this the world's longest law review footnote. However, some of the major criticisms include Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy"*, 34 VAND. L. REV. 1289, 1315 (1981); Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-first Century*, 65 IND. L.J. 549, 564–66 (1990); Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229 (1983) (arguing that the third-party doctrine cases are incorrect because they focus on the rights of the guilty rather than the rights of the innocent); Scott E. Sundby, *"Everyman" 's Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1757–58 (1994).

Recent criticisms of the doctrine include CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 151–64 (2007); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211 (2006) (arguing that the major third-party doctrine cases were wrongly decided on several grounds); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3; Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975 (2007); Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 2007 UCLA J.L. & TECH. 1, 3–4 (advocating a "retooling" of the third-party doctrine for internet searches); Andrew J. DeFilippis, Note, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1092 (2006) (arguing that the Supreme Court should overrule the third-party doctrine).

most-criticized fourth amendment cases."[6] Wayne LaFave asserts in his influential treatise that the Court's decisions applying it are "dead wrong"[7] and "make[] a mockery of the Fourth Amendment."[8] The verdict among commentators has been frequent and apparently unanimous: The third-party doctrine is not only wrong,[9] but horribly wrong.[10] Even many state court judges have agreed: Over a dozen state Supreme Courts have rejected the doctrine under parallel provisions of their state constitutions.[11]

Remarkably, even the U.S. Supreme Court has never offered a clear argument in its favor. Many Supreme Court opinions have applied the doctrine; few have defended it. The closest the Court has come to justifying the doctrine has been its occasional assertion that people who disclose communications to a third party "assume the risk" that their information will end up in the hands of the police.[12] But assumption of risk is a result rather than a rationale: A person must assume a risk only when the Constitution does not protect it. Exactly *why* the Constitution does not protect information disclosed to third parties has been left unexplained.

This Article offers a defense of the third-party doctrine, and especially its most controversial applications. It argues that the doctrine serves two roles that critics have missed. The first and most important purpose is to maintain the technological neutrality of Fourth Amendment rules. Use of third parties has a substitution effect: It takes open and public portions of crimes and hides them from public observation. Without the third-party doctrine, savvy wrongdoers could use third-party services in a tactical way to enshroud the entirety of their crimes in zones of Fourth Amendment protection. The result would allow technology to upset the Fourth Amendment's traditional balance between privacy and security, weakening the deterrent and retributive goals of criminal punishment. The third-party doctrine blocks this end-run around the traditional Fourth Amendment balance. It

---

6. Clark D. Cunningham, *A Linguistic Analysis of the Meanings of 'Search' in the Fourth Amendment: A Search for Common Sense*, 73 IOWA L. REV. 541, 580 (1988).

7. 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.7(c), at 747 (4th ed. 2004).

8. *Id.* § 2.7(b), at 736 ("Such a crabbed interpretation of the *Katz* test makes a mockery of the Fourth Amendment.").

9. *See* sources cited *supra* note 5.

10. *See, e.g.*, 1 LAFAVE, *supra* note 7, § 2.7(c), at 747 ("The result reached in *Miller* is dead wrong, and the Court's woefully inadequate reasoning does great violence to the theory of Fourth Amendment protection which the Court had developed in *Katz*."); Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 753 (2005) ("The third party doctrine presents one of the most serious threats to privacy in the digital age.").

11. For a list of states that have rejected the doctrine, in whole or in part, see Stephen E. Henderson, *Learning from All Fifty States: How To Apply the Fourth Amendment and Its State Analogs To Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373 (2006).

12. Smith v. Maryland, 442 U.S. 735, 744 (1979) ("Because the depositor [in *Miller*] 'assumed the risk' of disclosure, the Court held that it would be unreasonable for him to expect his financial records to remain private.").

helps ensure that the Fourth Amendment rules that apply to crimes committed using third parties are roughly equivalent to the rules that apply to crimes committed without them.

The doctrine's second role is to provide ex ante clarity. Under the third-party doctrine, Fourth Amendment protection for information matches the Fourth Amendment protection for the environment in which it is stored. As a result, Fourth Amendment rules are determined by information's knowable location rather than its unknowable history. Absent the third-party doctrine, courts would face the difficult challenge of creating a clear regime of Fourth Amendment protection for third-party information. Although such challenges are not insurmountable, the clarity of the third-party doctrine provides an important argument in its favor.

The third-party doctrine is no panacea, of course. Critics have made two important arguments against it, one doctrinal and the other functional.[13] The doctrinal argument is that the Justices do not understand the privacy interests at stake in third-party information. To these critics, the Justices' assertion that disclosure automatically renders an expectation of privacy "unreasonable" is simply incorrect.[14] The second argument is functional: It contends that the doctrine is misguided because it grants governments the authority to take more invasive steps without constitutional oversight than are consistent with a free and open society. In particular, the third-party doctrine gives government officials too much power to harass individuals in bad faith.[15]

This Article explains that while both criticisms have some appeal, both considerably overstate the case and ignore important counterarguments. Assertions that the Justices do not understand privacy are objections more about form than substance. Although the third-party doctrine has been framed in terms of the "reasonable expectation of privacy" test, it is better understood as a consent doctrine. Disclosure to third parties eliminates protection because it implies consent. When understood as a subset of consent law rather than an application of the reasonable expectation of privacy test, the third-party doctrine fits naturally within the rest of Fourth Amendment law.

Finally, functional arguments about government power overlook the legal system's substitutes for Fourth Amendment protection. The Fourth Amendment is not the only game in town. Common law privileges, entrapment law, the *Massiah* doctrine, First Amendment doctrine, and statutory privacy protections have been designed specifically to address concerns of police harassment in their use of third parties.[16] These mostly nonconstitutional legal principles each regulate specific aspects of third-party practices to deter police abuses, generally forcing the police to use third parties in good faith or

---

13. *See infra* Section I.B.

14. *See infra* Section I.B.1.

15. *See infra* Section I.B.2.

16. All of these doctrines are discussed *infra* Section IV.B.

in a reasonable way. Critics have overlooked these substitutes, and as a result have tended to see the choice as between Fourth Amendment protection or no protection at all. Understanding how other doctrines substitute for Fourth Amendment protection reveals that this understanding is incorrect.

The goal of this Article is to replace the partial view of the third-party doctrine found in existing scholarship with a richer and more balanced account of its costs and benefits. The topic is a timely one: Technological progress places more and more communications in the hands of third parties,[17] and the growing importance of new technologies such as the internet has led to a renewal of the attacks on the third-party doctrine.[18] Given the latest wave of criticisms, a more complete understanding is needed to better appreciate how the Fourth Amendment should apply both in the case of old technologies and new ones. I do not expect that the arguments offered in this Article will persuade every critic to change positions; reasonable people can disagree on whether the doctrine is appropriate in particular cases. At the same time, I hope the Article will demonstrate a strong affirmative argument for the doctrine in many cases and at least a plausible argument in others.

This Article proceeds in four parts. Part I briefly introduces the law of the third-party doctrine and the harsh criticisms of it. Part II argues that the third-party doctrine ensures technological neutrality of the Fourth Amendment by blocking the opportunistic use of third parties to circumvent the basic balance of Fourth Amendment rules. Part III contends that the doctrine is needed to provide ex ante clarity. The Fourth Amendment's suppression remedy requires clear rules governing when a Fourth Amendment search occurs, and the third-party doctrine creates that needed certainty. Part IV responds to the two primary criticisms of the third-party doctrine, that the doctrine is doctrinally unpersuasive and that it gives too much power to the police. It argues that the first claim is largely a matter of form and that the latter is addressed by legal rules beyond the Fourth Amendment.

I. Introduction to the Third-Party Doctrine

This Part explains the third-party doctrine and summarizes the two basic types of cases: those involving secret agents such as undercover informants, and those involving third-party account records. This Part also introduces the two primary criticisms of the third-party doctrine. The first criticism is doctrinal in nature; it asserts that it is simply incorrect to say that third-party exposure renders an expectation of privacy "unreasonable."[19] The second criticism is functional; it claims that the third-party doctrine gives the government too much power over individuals.[20]

---

17. *See* Solove, *supra* note 1, at 528–29.

18. *See, e.g.*, sources cited *supra* note 5.

19. *See infra* Section II.B.1.

20. *See infra* Section II.B.2.

A. *The Cases*

1. *Secret Agents, 1952–1971*

Although several of the Supreme Court's earliest cases in the law of criminal procedure involved the use of undercover agents and confidential informants[21]—so-called "secret agents"[22]—a Fourth Amendment challenge to such secret agents did not reach the Court until *On Lee v. United States*.[23] Lee sold opium from his laundry store and one day made incriminating statements to his friend Poy. It turned out that Poy was an undercover informant wearing a wire, and the recording of Lee's statements was used against Lee at trial. Lee argued that the government's conduct violated the Fourth Amendment because it was the equivalent of secretly placing a bug inside the store.

The Supreme Court disagreed. According to Justice Jackson, Lee simply "was talking confidentially and indiscreetly with one he trusted."[24] The fact that Poy was wearing a wire was irrelevant, because the recording was "with the connivance of one of the parties"[25] to the conversation (that is, Poy). Justice Jackson suggested that the very idea of seeing these facts as problematic under the Fourth Amendment was quite silly: "It would be a dubious service to the genuine liberties protected by the Fourth Amendment to make them bedfellows with spurious liberties improvised by farfetched analogies . . . ."[26]

The Court reached the same result a decade later in *Lopez v. United States*.[27] Lopez tried to bribe an IRS agent who was wearing a wire, and both the recording and the agent's testimony were admitted against Lopez at trial. Citing *On Lee*, Justice Harlan readily rejected Lopez's claim that his Fourth Amendment rights were violated: "Lopez knew full well [his statements] could be used against him by [the IRS agent] if he wished,"[28] and the wire recording "device was used only to obtain the most reliable evidence possible of a conversation in which the Government's own agent was a participant and which that agent was fully entitled to disclose."[29]

---

21. For example, in *Gouled v. United States*, 255 U.S. 298 (1921), a business acquaintance of a criminal suspect pretended to pay a social visit at the suspect's office when he in fact was intending to search the office for evidence. Eleven years later, in *Sorrells v. United States*, 287 U.S. 435 (1932), an undercover prohibition agent looking for alcohol gained entrance to a suspect's home by posing as a tourist. Although these cases involved secret agents, they did not specifically raise Fourth Amendment challenges to secret agents' use.

22. *See, e.g.*, YALE KAMISAR ET AL., MODERN CRIMINAL PROCEDURE 465 (12th ed. 2008).

23. 343 U.S. 747 (1952).

24. *Id.* at 753.

25. *Id.* at 754.

26. *Id.*

27. 373 U.S. 427 (1963).

28. *Id.* at 438.

29. *Id.* at 439.

Lopez was followed quickly by *Lewis v. United States*[30] and *Hoffa v. United States*,[31] handed down the same day in 1966. In *Lewis*, the defendant invited an undercover agent into his home to sell him marijuana. In *Hoffa*, Teamsters President Jimmy Hoffa confided in his colleague Partin, who turned out to be working secretly for the police. In both cases, the secret agents later testified about what they had seen and heard. Relying on *Lopez* and *On Lee*, the Court concluded that neither use of secret agents had violated the Fourth Amendment. While Hoffa "was relying upon his misplaced confidence that Partin would not reveal his wrongdoing," the Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."[32] And use of an undercover officer in *Lewis* could not be unconstitutional because such a rule would severely hamper undercover investigations:

> Were we to hold the deceptions of the agent in this case constitutionally prohibited, we would come near to a rule that the use of undercover agents in any manner is virtually unconstitutional *per se*. Such a rule would, for example, severely hamper the Government in ferreting out those organized criminal activities that are characterized by covert dealings with victims who either cannot or do not protest.[33]

The last of the secret agent cases, *United States v. White*,[34] affirmed that the third-party doctrine survived the formal switch to the reasonable expectation of privacy test first articulated in Justice Harlan's concurrence in *Katz v. United States*.[35] The facts of *White* were almost identical to those of *Lopez*: White spoke about his crimes to an undercover informant who was wearing a wire, and the recordings of the conversations were used against him at trial.[36] The plurality opinion by Justice White concluded that *Hoffa*, *Lopez*, and *On Lee* had survived *Katz*.[37] *Katz* did not disturb that line of cases because it "involved no revelation to the Government by a party to conversations with the defendant."[38] In the language of *White*, an expectation that a person would not share private information with the police was not constitutionally justifiable:

> Inescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police. If he sufficiently doubts their trustworthiness, the association will very probably end or never

30. 385 U.S. 206 (1966).

31. 385 U.S. 293 (1966).

32. *Id.* at 302.

33. *Lewis*, 385 U.S. at 210.

34. 401 U.S. 745 (1971).

35. 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

36. *White*, 401 U.S. at 746–47.

37. *Id.* at 749–50.

38. *Id.* at 749. Because Justice Black's concurring opinion adopted a far broader rationale, Justice White's plurality opinion expresses the holding of the Court.

> materialize. But if he has no doubts, or allays them, or risks what doubt he has, the risk is his.[39]

Exactly *why* this conclusion was "inescapable"—and why "the risk is his"—was left unexplained.

2. *Business Records, 1973–1980*

The second round of third-party doctrine cases occurred from 1973 to 1980, and they all involved various types of business records. In all of the cases, the Court held that transferring business records to third parties relinquished Fourth Amendment protection. In *Couch v. United States*,[40] Couch had given tax documents to his accountant, and the government issued an IRS summons ordering the accountant to hand over documents that related to Couch's tax returns.[41] In *United States v. Miller*,[42] the government served subpoenas on banks used by the defendant Miller seeking all records relating to his accounts. In *United States v. Payner*,[43] investigators stole a briefcase owned by the vice president of a bank in the Bahamas and then copied the briefcase's contents before returning it. The contents revealed that Payner maintained an account at the bank, and this helped the government show that Payner had falsified his tax returns.[44]

In all three cases, the defendant moved to suppress the financial records under the Fourth Amendment. In all three cases, the Court rejected the claims under the third-party doctrine in opinions by Justice Powell. In *Couch*, Justice Powell concluded that "there can be little expectation of privacy where records are handed to an accountant."[45] By handing information to his accountant, Couch had given his accountant the power to decide what information would be further disclosed in Couch's income tax returns.[46] In *Miller*, Justice Powell used two different arguments. First, the bank records were not the defendant's private or personal letters, but rather were financial documents that would be used in the ordinary course of business.[47] Second, the defendant had voluntarily conveyed the information to a third party just like White, Hoffa, and Lopez. "[I]n revealing his affairs to another," the defendant had assumed the risk "that the information [would] be conveyed by

---

39. *Id.* at 752.

40. 409 U.S. 322 (1973).

41. *Id.* at 324–25.

42. 425 U.S. 435 (1976).

43. 447 U.S. 727 (1980).

44. *Id.* at 728–30.

45. *Couch*, 409 U.S. at 335.

46. *See id.* ("What information is not disclosed is largely in the accountant's discretion . . . . Indeed, the accountant himself risks criminal prosecution if he willfully assists in the preparation of a false return. His own need for self-protection would often require the right to disclose the information given him." (citation omitted)).

47. *Miller*, 425 U.S. at 442.

that person to the Government."[48] In *Payner*, Justice Powell found the case indistinguishable from *Miller*.[49]

Finally, the Court applied the third-party doctrine in *Smith v. Maryland*,[50] a case involving pen registers. A pen register was a device installed at the phone company to record the numbers dialed from a specific telephone. In *Smith*, investigators had asked the phone company to install a pen register on the home phone of a man suspected of robbing and then harassing a woman by making anonymous phone calls. The pen register confirmed that the calls were originating from the man's home, and that information was used to help get a warrant to search his home.[51] The Supreme Court held that use of the pen register was not a "search" because it was covered by the third-party doctrine: "When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed."[52] According to Justice Blackmun, writing for the majority, "[t]he switching equipment that processed those numbers [was] merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber."[53] The third-party doctrine applied even though "the telephone company ha[d] decided to automate."[54]

B. *Common Criticisms of the Third-Party Doctrine*

The criticisms of the third-party doctrine derive from two basic arguments, one doctrinal and the other functional. Both arguments were first developed in dissents from the important third-party doctrine cases, most notably Justice Harlan's dissent in *White*[55] and Justice Marshall's dissent in *Smith*.[56] In the decades since these opinions, a large body of scholarship has echoed and expanded on their two basic claims.

1. *The Doctrinal Critique*

The first important criticism of the third-party doctrine is that it does not accurately apply the reasonable expectation of privacy test. According to

48. *Id.* at 443.

49. *Payner*, 447 U.S. at 732 ("*United States v. Miller* established that a depositor has no expectation of privacy and thus no protectable Fourth Amendment interest in copies of checks and deposit slips retained by his bank. Nothing in the record supports a contrary conclusion in this case." (citations omitted) (internal quotation marks omitted)).

50. 442 U.S. 735 (1979).

51. *Id.* at 737.

52. *Id.* at 744.

53. *Id.*

54. *Id.* at 745.

55. United States v. White, 401 U.S. 745, 768–95 (1971) (Harlan, J., dissenting).

56. *Smith*, 442 U.S. at 748–52 (Marshall, J., dissenting).

critics, individuals normally expect privacy in their bank records, phone records, and other third-party records.[57] Such expectations of privacy are common and reasonable, and Justices who cannot see that are simply out of touch with society and are misapplying the Fourth Amendment.[58] From this perspective, it "defies reality"[59] to say that a person "voluntarily" surrenders information to third parties like banks or telephone companies.[60] As Justice Marshall reasoned in his *Smith* dissent, "[i]t is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative."[61]

A corollary to this claim is that the Justices supporting the third-party doctrine have misunderstood the concept of privacy. The Justices envision privacy as an on-off switch, equating disclosure to one with disclosure to all, and as a result they miss the many shades of gray.[62] As Justice Marshall put the point in *Smith*, "[p]rivacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[63] Echoing Justice Marshall, Daniel Solove argues that the third-party doctrine is based on an incorrect "conception of privacy," a conception of privacy as total secrecy.[64] Along the same lines, Richard Posner argues that the *Miller* line of cases is "unrealistic."[65] "Informational privacy does not mean refusing to share information with everyone," he maintains, for "[o]ne must not confuse solitude with secrecy."[66] Sherry Colb agrees, writing that "treating exposure to a limited audience as identical to exposure to the world"[67] fails to recognize the degrees of privacy.

---

57. *See, e.g.*, Ashdown, *supra* note 5, at 1315 ("[T]elephone patrons undoubtedly would be shocked to learn that records of their calls either were available for third parties or were being distributed outside the telephone system."); Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society"*, 42 DUKE L.J. 727, 732 (1993) (arguing that some Supreme Court cases "do not reflect societal understandings" of when an expectation of privacy is "reasonable," and that "some of the Court's conclusions [about what expectations of privacy are reasonable] may be well off the mark").

58. *See* Slobogin & Schumacher, *supra* note 57, at 732.

59. Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 829 (2005).

60. *See also* Ashdown, *supra* note 5, at 1315.

61. *Smith*, 442 U.S. at 750 (Marshall, J., dissenting).

62. *See, e.g.*, Katz, *supra* note 5, at 564–66.

63. *Smith*, 442 U.S. at 749 (Marshall, J., dissenting).

64. Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1086 (2002).

65. RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY 140 (2006).

66. *Id.*

67. Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122 (2002).

2. *The Functional Critique*

The second major critique of the third-party doctrine contends that it gives the government more power than is consistent with a free and open society. The first significant elaboration of this argument appears to be Justice Harlan's dissent in *United States v. White*.[68] Harlan argued that the government should not be permitted to use an undercover informant with a wire because leaving such a procedure unregulated would grant the government too much power:

> Were third-party bugging a prevalent practice, it might well smother that spontaneity—reflected in frivolous, impetuous, sacrilegious, and defiant discourse—that liberates daily life. Much off-hand exchange is easily forgotten and one may count on the obscurity of his remarks, protected by the very fact of a limited audience, and the likelihood that the listener will either overlook or forget what is said, as well as the listener's inability to reformulate a conversation without having to contend with a documented record. All these values are sacrificed by a rule of law that permits official monitoring of private discourse limited only by the need to locate a willing assistant.[69]

Justice Marshall's dissent in *Smith*[70] made a similar point. According to Marshall, exempting pen registers from Fourth Amendment scrutiny enabled unregulated monitoring that would be harmful to a free society:

> The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide. Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts. Permitting governmental access to telephone records on less than probable cause may thus impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society.[71]

Arnold Loewy picked up this theme in his 1983 article, *The Fourth Amendment as a Device for Protecting the Innocent*.[72] Loewy posited that Fourth Amendment protections should protect the innocent, and then reasoned that the third-party doctrine cases gave the police too much power to harass innocent citizens.[73] By allowing undercover agents to record suspects without judicial scrutiny, the Court had given them "the ability to use [the recordings] for parlor games, practical jokes, or harassment."[74] By allowing the police to install pen registers without oversight, the Court had left the

68. 401 U.S. 745 (1971).

69. *See id.* at 787–89 (Harlan, J., dissenting) (footnotes omitted).

70. Smith v. Maryland, 442 U.S. 735, 748–52 (1979) (Marshall, J., dissenting).

71. *Id.* at 751 (citations omitted).

72. Loewy, *supra* note 5.

73. *Id.* at 1252–56.

74. *Id.* at 1253.

police "perfectly free to learn every telephone number that any persons [sic] dials, subject only to the cooperation of the telephone company."[75]

Other scholars have made similar points,[76] often in discussions of how the Fourth Amendment applies to computers and the Internet. Internet services are third-party services, raising the prospect that the Fourth Amendment may apply only modestly to internet communications. Scholars have responded by contending that the third-party doctrine is "not responsive to life in the modern Information Age."[77] If third-party services play a growing role in government surveillance, the concern runs, then the Fourth Amendment will regulate a smaller and smaller portion of that surveillance; the government will be able to collect and assemble "digital dossiers" without Fourth Amendment scrutiny.[78] To ensure sufficient constitutional protection online, many argue, the third-party cases should be overruled or sharply limited to their facts.[79]

II. Substitution Effects and the Functional Role of the Third-Party Doctrine

The widespread criticism of the third-party doctrine overlooks two important benefits of the rule. This Part explains the first major benefit of the third-party doctrine: It ensures technological neutrality in Fourth Amendment rules. The use of third parties has a substitution effect. It enables wrongdoers to take public aspects of their crimes and replace them with private transactions. Without a third-party doctrine, suspects can act opportunistically to effectively hide their criminal enterprises from observation. The result upsets the basic balance of Fourth Amendment law, undercutting the deterrent and retributive force of criminal law. The third-party doctrine blocks such efforts, resulting in a rough equivalence in the overall amount of privacy for criminals acting alone and the amount of privacy for those using third parties.

To develop this argument, I will start with the basic balance of the Fourth Amendment. I will explain how third parties threaten this balance and how the third-party doctrine retains it. I will then cover a few examples

---

75. *Id.* at 1255.

76. *See, e.g.*, Katz, *supra* note 5, at 568–69 ("The government is free from any judicial oversight. Without a reasonableness limitation, we must rely on government officials to voluntarily respect our privacy.").

77. Solove, *supra* note 64, at 1087.

78. *Id.*; Joseph T. Thai, *Is Data Mining Ever a Search Under Justice Stevens's Fourth Amendment?*, 74 Fordham L. Rev. 1731, 1736–45 (2006).

79. *E.g.*, Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 Geo. Wash. L. Rev. 1375, 1403 (2004) (articulating that the third-party doctrine should be construed narrowly in the context of computer and internet communications); Freiwald, *supra* note 5, at ¶ 40; Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 Geo. Wash. L. Rev. 1557 (2004) (arguing that the third-party doctrine should be read narrowly in the case of computer and internet communications).

and conclude by showing how the doctrine is an essential aspect of the technological neutrality of Fourth Amendment rules.

A. *The Basic Division of the Fourth Amendment*

The Fourth Amendment's prohibition on unreasonable searches and seizures is premised on a balance between privacy and security. To implement that balance, the Supreme Court has created two basic categories of law enforcement conduct: investigative steps that the Fourth Amendment regulates and those that it does not. Under this scheme, the Fourth Amendment protects some things and some places while leaving others open to government surveillance. For example, the Fourth Amendment protects a person's home and private packages.[80] If the government wants access to those places, it must ordinarily have a search warrant.[81] On the other hand, occurrences in public or on open fields are not protected by the Fourth Amendment.[82] If the government wants to monitor such spaces, the Fourth Amendment does not interfere: The monitoring is not a search or seizure.

The Fourth Amendment's divide between unregulated and regulated spaces forms an essential part of how the amendment works. It divides evidence collection into two stages: less invasive steps the government can take at any time, and more invasive steps the government can only take when it has already collected enough evidence to demonstrate special conditions such as probable cause or exigent circumstances. From an investigative standpoint, the two categories work together. Investigations often start with the open surveillance, permitting the police to look for clues that may indicate criminal activity. If the open surveillance yields sufficient evidence, that evidence permits the government to take more invasive steps that are often necessary to prove cases beyond a reasonable doubt in court.[83]

The basic division into unregulated and regulated steps leads to a balance between privacy and security because most crimes have traditionally required suspects to carry out at least part of their crimes in spaces open to surveillance. To see why, consider a world with no advanced technology. Part of the crime will normally occur outside. If John wants to rob a person walking down the street, for example, he needs to leave his house and go out to the street. If he wants to purchase drugs, he needs to go out of his home and find a dealer who will sell them to him. If he wants to murder his coworker, he needs to go out and buy a knife; after the act, he needs to dispose

---

80. *E.g.*, Payton v. New York, 445 U.S. 573, 585 (1980) (noting that the " 'chief evil against which the Fourth Amendment is directed' " is the warrant-less entry and search of a home (quoting United States v. United States Dist. Court, 407 U.S. 297, 313 (1972))).

81. *Id.*

82. California v. Ciraolo, 476 U.S. 207, 213 (1986) ("The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares.").

83. In the argot of existing doctrine, government conduct that violates a reasonable expectation of privacy is a "search" that ordinarily triggers the warrant requirement; other government conduct is not a "search" at all.

of the body. In all of these traditional types of crimes, the wrongdoer has to leave his home and go out into spaces unprotected by the Fourth Amendment.

The public component of most traditional crimes is critical to the traditional balance of Fourth Amendment rules. If at least part of a crime occurs in spaces unprotected by the Fourth Amendment, the police have at least some opportunity to look more closely at whether criminal activity is afoot. Because the police normally begin an investigation with only speculation that a particular person is a lawbreaker, the public portion of crimes give the police an opportunity to develop more evidence. The police will have access to the public portion of the crime free of legal regulation. If they are observing him, they will know where the suspect went and what he said in public. That information won't solve the crime in most cases: Unless an officer directly observes the crime, the publicly available evidence only provides a lead.[84] But it's a start. If the evidence is strong enough, it can support invasions of protected spaces with a warrant. And those steps help the police solve at least a moderate percentage of criminal cases. Of course, many cases won't be solved. But enough cases are solved that a significant prospect of criminal punishment exists, allowing the criminal justice system to serve its utilitarian and retributive ends.

B. *Third Parties and the Basic Division*

Third parties pose a major threat to the Fourth Amendment's basic division between unregulated and regulated steps. The reason is that third parties act as remote agents that permit wrongdoers to commit crimes entirely in private. Those committing crimes naturally try to hide them from the police; no criminal wants to get caught. If a wrongdoer can use third parties as remote agents, he can reduce his exposure to public surveillance. Instead of going out into the world and subjecting himself to exposure, a wrongdoer can bring third-party agents inside and share plans or delegate tasks to them. He can use the third-party services to commit his crimes without exposing himself to spaces open to government surveillance.

Put another way, the use of third parties often has a *substitution effect*.[85] Without the third party, the wrongdoer would have needed to go out into public spaces where the Fourth Amendment does not regulate surveillance. But use of a third party substitutes a hidden transaction for the previously open event. What would have been public now becomes hidden. The wrongdoer no longer needs to leave his home, as the third-party agents

---

84. Of course, this is not true in every case: It is possible to imagine an entirely private crime such as attempting suicide. But in most cases, some exposure is necessary.

85. In economics, a "substitution effect" generally refers to change in the amount of a product consumed if the relative price of a competing product is raised. The concept of a substitution effect can be applied more broadly, however, to show how two different means of committing a crime can compete with each other. *See, e.g.*, Neal Kumar Katyal, *Deterrence's Difficulty*, 95 MICH. L. REV. 2385, 2387 (1997) (applying the substitution effect framework to criminal conduct).

enable him to commit the crime remotely. The crime now comes to the criminal rather than the criminal going to the crime.[86]

Consider how a person might use third parties to commit crimes from the protection of his own home. A mob boss might summon his underlings to his house to give them orders. A stalker might call his victim on his home phone rather than lying in wait outside her door. A computer hacker might hack into computers thousands of miles away without leaving his bedroom. In all of these cases, individuals use third parties to carry on their crimes without exposing themselves to spaces unprotected by the Fourth Amendment. The third-party agents—the employee, the telephone, and the Internet—do the work remotely on the principal's behalf.

Now we can see the importance of the third-party doctrine. Without the doctrine, criminals could use third-party agents to fully enshroud their criminal enterprises in Fourth Amendment protection. A criminal could plot and execute his entire crime from home knowing that the police could not send in undercover agents, record the fact of his phone calls, or watch any aspect of his Internet usage without first obtaining a warrant. He could use third parties to create a bubble of Fourth Amendment protection around the entirety of his criminal activity.

The result would be a notable shift in the balance between privacy and security. If any observation of any part of the target's conduct violates his reasonable expectation of privacy, then the police would need a warrant to observe any aspect of his behavior. That is, they would need probable cause to believe that the evidence to be collected constitute evidence of the crime. But if the entire crime were protected by a reasonable expectation of privacy, they couldn't observe any aspect of the crime to develop that probable cause. The effect would be a Catch-22: The police would need probable cause to observe evidence of the crime, but they would need to observe evidence of the crime first to get to probable cause. In many cases, this would eliminate the use of third-party evidence in investigations altogether. By the time the police would have probable cause to believe that someone's third-party records are evidence of crime, they usually would already have probable cause to arrest and charge him with the crime.[87]

What privacy on mobile phone data? – outside home but lots of data!

I don't like this argument

86. Further, the ability to harness outsourcing tools also often comes with a capacity to minimize the risk of betrayal. Criminals can control those in whom they confide, selecting only the most trustworthy to tell criminal secrets. The mob boss might require all his minions to prove their loyalty to him through deeds or a loyalty oath. The hacker will pick an Internet Service Provider that promises it will never under any circumstances cooperate with the police. For a rational criminal, all these steps make good sense. By only proceeding when the risk of betrayal is low, the criminal ensures the greatest chance of success for his criminal enterprise.

87. For investigators to obtain a probable cause warrant, they must establish ex ante a "fair probability" that evidence of the crime is located in the specific place the police wish to access. And "fair probability" ex ante turns into a high probability ex post: Studies have found that warrants prove successful—revealing the evidence sought—in the clear majority of cases. *See* RICHARD VAN DUIZEND ET AL., THE SEARCH WARRANT PROCESS 39 tbl.22 (1985) (reporting that warrants executed by the police yielded most or all of the items listed on the warrant in between sixty-four and eighty-two percent in the seven jurisdictions studied). Police will have such leads at the outset of investigations only rarely. In most cases they will begin with a victim's report or a crime scene or an anonymous tip; establishing probable cause about a particular wrongdoer and particular evidence

The third-party doctrine responds with a rule that ensures roughly the same degree of privacy protection regardless of whether a criminal commits crimes on his own or uses third parties. The part of the crime that previously was open to observation—the transaction itself—remains open to observation. The part of the crime that previously was hidden—what the suspect did without third parties in his home—remains hidden. The result leaves the Fourth Amendment rule neutral as to the means of committing the crime: Using a third party does not change the overall level of Fourth Amendment protection over the crime. If a person commits a crime on his own, the open part of the crime may be observed by the police without a warrant. If he harnesses a third party, the third party's involvement is treated as open, resulting in roughly the same amount of open conduct as the self-executed crime.

C. *Examples*

Examples help demonstrate how third parties create a substitution effect and how the third-party doctrine maintains the same degree of privacy protection regardless of whether third parties are used. In particular, consider the two most controversial applications of the third-party doctrine: the pen register installed in *Smith v. Maryland*,[88] and the bank account records retrieved in *United States v. Miller*.[89]

1. Smith v. Maryland—*Pen Registers*

Recall that in *Smith v. Maryland*,[90] Smith harassed a robbery victim by calling her repeatedly on the telephone. The police suspected Smith, and they asked the phone company to install a pen register device that would note any outgoing calls from his home phone. The pen register recorded the fact of the call to the victim, suggesting that Smith was the harasser and helping to provide the police with probable cause for a warrant to search his home.

To understand the substitution effect here, we need to see exactly how Smith used the third party of the telephone system to eliminate the public aspect of his crime. In a world without a telephone system, Smith would have been forced to stalk his victim the old-fashioned way. Smith would have left his house, walked to his car, and driven to his victim's home to harass her in person. Instead of having the phone company install a pen register, the police

---

requires a great deal of additional leads. Under the third-party doctrine, the police have many tools that they can use without probable cause to reach the probable cause threshold. They can ask around; they can go undercover; they can get bank records. Those tools may help prove the probable cause needed to obtain a warrant to search a home or to make an arrest. But if those tools *themselves* require probable cause, then in a practical sense those tools are no longer available to officers to help solve investigations.

88. 442 U.S. 735 (1979).

89. 425 U.S. 435 (1976).

90. *Smith*, 442 U.S. at 737–38.

would have assigned an officer to watch Smith from public streets and "tail" him around town. The officer would have watched Smith leave his home, enter his car, and drive to the victim's house.

When we introduce the third party of the telephone system, however, Smith no longer needs to leave home. To borrow from the old advertising campaign for the Yellow Pages, he can "let [his] fingers do the walking."[91] What formerly would have occurred in the open air now takes place inside the home using the third party of the telephone. Instead of watching Smith in public, the police now need to install a pen register to get the equivalent of the previously public information about what he was doing.

From this perspective, the Supreme Court's decision in *Smith v. Maryland* properly blocks Smith's attempted end-run around the balance of Fourth Amendment rules. Its conclusion that installation of the pen register is not a search matches the Fourth Amendment protection for third-party crimes to the preexisting protection for solo crimes. Smith's use of a third party withdrew his identity from public surveillance. Instead of having to travel to his victim, the telephone brought his victim to him (virtually, at least). The pen register information substituted for the same information that the police would have obtained by watching Smith on the public street. Smith's physical presence was not protected in the physical world version of the crime; under the third-party doctrine, his virtual presence is not protected in the third-party environment of the telephone network.[92]

2. United States v. Miller—*Bank Records*

Next consider *United States v. Miller*,[93] and its finding of no Fourth Amendment protection for bank records. The substitution effect is somewhat harder to see in this case, but I think it still explains the outcome. In *Miller*, the government wanted to prove that Miller had set up an illegal alcohol still. Prosecutors used Miller's bank records to show that he had purchased equipment for the still using his checking account.[94] In other words, the government used the checking account to prove a trade: Miller's

91. Paul R. La Monica, *Let your fingers do the walking*, CNNMONEY.COM, December 13, 2005, http://money.cnn.com/2005/12/13/news/fortune500/yellow.

92. During the editing stage, I learned that Ric Simmons recently made a similar argument about *Smith*. *See* Ric Simmons, *Why 2007 Is Not Like* 1984*: A Broader Perspective on Technology's Effect on Privacy and Fourth Amendment Jurisprudence*, 97 J. CRIM. L. & CRIMINOLOGY 531, 553–54 (2007). Simmons and I share a similar approach to how technology impacts Fourth Amendment protection; both of us have emphasized how technological change can both take away government power and expand it, and how Fourth Amendment rules respond to changes in both directions. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 864–67 (2004); Simmons, *supra*, at 535–36. Simmons ultimately condemns the third-party doctrine, calling it "dangerously short-sighted," but that is because he assumes that the doctrine must also apply to the contents of communications. Simmons, *supra*, at 555. As I explain in Section II.D, I do not think the third-party doctrine needs to apply to contents of communications. With that caveat, I agree with the basic approach of Professor Simmons.

93. 425 U.S. 435 (1976).

94. Specifically, Miller had written a check to rent a van and purchase radio equipment, sheet metal, and metal pipe. *See id.* at 438.

cash, drawn from the bank, in exchange for the items he was purchasing to build the still. The Supreme Court held that the Fourth Amendment did not protect Miller's bank records; specifically, it did not protect from government scrutiny the checks Miller had to written make those trades.[95]

In *Miller*, the checking account created a substitution effect by replacing a transaction that would have included substantial public components with a transaction that would normally occur entirely in private. To see how, imagine a world without banks. If you need to pay for something in this world, you would need to get the money to do it: You would need to travel to your stash, pick up the money, and then travel to the place where you are making your purchase. If you are the seller, you need to receive the money, take it back to your stash, and store it away for safekeeping. There are public parts of the transaction on both sides. Checks and other credit instruments eliminate the need to travel. The buyer no longer needs to travel to bring the money to the seller, and the seller no longer needs to travel to put the money away. Instead, the seller deposits the check and the funds from the bank are sent directly to him. The buyer and seller don't have to move anymore, as the check moves the funds out of and into their accounts without them needing to go anywhere. The third party of the checking account makes the entire economic transaction private.

Use of the third-party doctrine in the *Miller* case is plausible because checking services replace significantly public transactions with private ones. The third-party doctrine ensures that the same Fourth Amendment rules apply to checking account transactions that would have applied to the public transactions that they replace.

D. *Third Parties and Technology Neutrality*

I recognize that the model above is a bit artificial. It imagines a mythical year zero in which no third parties existed, whether of the human or mechanical type. Obviously, no such time existed. The model above also imagines that the substitution effect will occur equally in every case. It won't: Criminals can use third parties to withdraw the public portion of their crimes, but they certainly don't have to do so. In the *Smith* case, for example, Smith could have placed his anonymous stalking call from a public pay phone with the door open; or, in the modern equivalent, he could have used a cell phone in a crowded city street and spoken loudly so all could hear. If he had done this, using a third party would not have altered the open aspect of the crime.

---

95. The *Miller* court explained:

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.

Id. at 443 (citations omitted).

At the same time, the somewhat simplified model reveals an essential dynamic about the use of third parties: In general, the use of a third party can create a substitution effect where the wrongdoer wishes it to do so. Hoffa could choose to speak only to close colleagues in the safety of his hotel room; Smith could choose to call his victim only from his own home phone. Use of a third party does not always have a substitution effect, but it enables the effect at the suspect's option. And any smart criminal will exercise the option. Those who have the most to hide have the most incentive to take advantage of how third-party services can hide their activity. Even without Fourth Amendment rules, third-party services will tend to hide otherwise public transactions. A rational actor bent on criminal conduct will use as many third-party services as he can to avoid detection.

Viewed from this perspective, the third-party doctrine is not some sort of mysterious hole in Fourth Amendment protection. To the contrary, it is a natural analog to the Supreme Court's decision in *Katz v. United States*.[96] *Katz* effectively required technological neutrality: Although its precise reasoning is opaque, it is often understood as concluding that telephone calls are protected because of the function they serve rather than the accident of the technology they use.[97] Indeed, this was the basic rationale of Justice Brandeis's dissent in *Olmstead v. United States*.[98] Brandeis feared that technological change could narrow Fourth Amendment protection: "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."[99] Brandeis proposed that the Fourth Amendment should keep up as technology changed so that new technologies would not gut privacy.

But if we embrace this understanding of the Fourth Amendment, then surely it must be a two-way street. Just as the new technologies can bring "intimate occurrences of the home" out in the open, so can technological change and the use of third parties take transactions that were out in the open and bring them inside. If we accept that the Fourth Amendment should stay technology neutral, then we should accept that rule both when new technological practices threaten to expand Fourth Amendment protection as when they threaten to constrict it. Just as the Fourth Amendment should protect that which technology exposes, so should the Fourth Amendment permit access to that which technology hides. From this perspective, the third-party doctrine is needed to ensure the technology neutrality of the Fourth

96. 389 U.S. 347 (1967).

97. The *Katz* Court stated:

> One who occupies [a phone booth], 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.

Id. at 352.

98. 277 U.S. 438, 471 (1928) (Brandeis, J., dissenting).

99. *Id.* at 474.

Amendment. It ensures that we have the same rough degree of Fourth Amendment protection independently of whether wrongdoers use third-party agents to facilitate their crimes.

More broadly, the third-party doctrine in no way undermines *Katz*, which famously held that the contents of a call from a public telephone receive Fourth Amendment protection. The contents of communications sent over third-party networks do not trigger substitution effects: The use of the network does not hide contents that previously were open. When a person visits another in his home, the fact of the visit occurs in public but the actual contents of their conversations remain shielded from observation. Extending the Fourth Amendment to contents of communications but excluding address information—as the Supreme Court did in *Katz* and *Smith*—maintains that status quo and follows a technologically neutral approach to constitutional protection.

III. The Third-Party Doctrine and Ex Ante Clarity

The second important role of the third-party doctrine is to foster ex ante clarity in Fourth Amendment rules. The on/off switch of the suppression remedy demands clear Fourth Amendment rules on what police conduct triggers Fourth Amendment protection and what police conduct does not.[100] The third-party doctrine creates ex ante clarity by matching the Fourth Amendment rules for information with the Fourth Amendment rules for location. Under the doctrine, rights in information extinguish when the information arrives at its destination. This means that the present location of information defines the Fourth Amendment rules for collecting it, and the Fourth Amendment rules are constant within each location.

Without the third-party doctrine, courts would have to develop some alternative test, with the same ex ante clarity, for identifying when information is protected under the Fourth Amendment. This task may not be impossible, but it is quite difficult. Few critics of the third-party doctrine have tried. And the difficulty of devising a clear alternative to the third-party doctrine provides a second argument in its favor.

A. *Ex Ante Clarity Under the Third-Party Doctrine*

To understand the importance of ex ante clarity, it is essential to recognize that the exclusionary rule provides the primary mechanism for enforcing the Fourth Amendment.[101] If the police violate a reasonable expectation of privacy and no exception applies, the evidence obtained ordinarily

---

100. *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 Stan. L. Rev. 503, 527 (2007) ("The Fourth Amendment's suppression remedy . . . generates tremendous pressure on the courts to implement the Fourth Amendment using clear ex ante rules rather than vague ex post standards.").

101. *See id.* at 527–28.

will be suppressed and the wrongdoer may go free.[102] The severe costs of the exclusionary rule require ex ante clarity in the rules for when a reasonable expectation of privacy exists. The police need to know when their conduct triggers Fourth Amendment protection. Uncertainty can both overdeter police from acting when no protection exists and can lead them to inadvertently trample on Fourth Amendment rights.[103]

The third-party doctrine ensures ex ante clarity by matching the Fourth Amendment rules for collecting information with the location of the information collected. When information arrives at its destination, the Fourth Amendment rules for collecting the information match with the rules for collecting other evidence there. This is true because rights in information extinguish when the information arrives at its destination; the information has been disclosed to its recipient, and any preexisting Fourth Amendment protection no longer exists.[104] This approach is essential to the clarity of Fourth Amendment rules because it guarantees that once information is present in a location it is treated just like everything else located there. Because the history of information is erased when it arrives, the law can impose rules as to what the police can or cannot do based on the known location of the search instead of the unknown history of the information obtained.

Consider a letter that arrives in the mail, is opened, and sits on the recipient's desk at home in a stack of other letters and other papers. The third-party doctrine dictates that the letter is treated just like all the other papers on the desk. The sender has Fourth Amendment rights in the letter during transmission, but once it arrives at its destination, those rights disappear.[105] If the police wish to search the home and come across a stack of papers including the letter, the Fourth Amendment rules they must follow will be set by the usual rules of home searches rather than special rules for each piece of paper defined by the history of each page. By erasing the history of information for Fourth Amendment purposes, the third-party doctrine ensures that all information in the same location is treated in the same way. This is critical because the police will normally know the status of the place they search but not the history of the items found inside it.

The significance of the ex ante clarity provided by the third-party doctrine is demonstrated by the surprising difficulty of developing alternatives to the doctrine that can retain that clarity. Under the third-party doctrine, if *A* tells a secret to *B*, *A* has no rights in *B*'s possession of the information. If the third-party doctrine is rejected, however, *A*'s rights in that information should continue even though *B* has the information now in addition to *A*. In other words, information should retain a history: The Fourth Amendment rules that apply to information should consider where the information has been in the past and in what circumstances it was held and disclosed. The

102. *See generally* Mapp v. Ohio, 367 U.S. 643 (1961) (applying the Fourth Amendment's suppression remedy to the states through the Fourteenth Amendment).

103. *See* Kerr, *supra* note 100, at 527–28.

104. *See supra* Section II.A.

105. *See* United States v. Villarreal, 963 F.2d 770, 774 (5th Cir. 1992).

question is, how far should those rights go? Should they extend forever? What should extinguish them? For the most part, the scholarly commentary has ignored this problem: Most scholars who criticize the doctrine do so without actually explaining what test should replace it.[106] But if it takes a theory to beat a theory, then surely it takes a doctrine to beat a doctrine. And it turns out to be quite difficult to devise a replacement for the third-party doctrine that would provide the needed clarity.

B. *Ex Ante Clarity Under a Probabilistic Alternative*

Because there are several different ways to determine when an expectation of privacy is reasonable,[107] it helps to consider two different alternatives to replace the third-party doctrine. One alternative is what I have termed the probabilistic model of Fourth Amendment protection.[108] Under this approach, whether government conduct violates a reasonable expectation of privacy depends on a fact-specific inquiry as to whether a reasonable person would have expected that the information would remain private.[109] This is a prospective inquiry from the standpoint of the suspect: The question is whether a reasonable person in the suspect's situation would expect the information to be widely disseminated. In this Section, I will explain why the probabilistic approach cannot create the needed clarity. A probabilistic approach would rest the inquiry on a largely unknowable question; the police would have difficulty applying the Fourth Amendment because they normally would be unable to reconstruct whether someone reasonably expected privacy in the information collected.

The core difficulty with applying a probabilistic approach to third-party information is that information's history is often complex and impossible to reconstruct. Just as a glass of water from a kitchen sink tap might have been rainwater in the Amazon thousands of years ago, information today often has a long past of interpersonal transmission. What a person knows and thinks reflects what he has seen, smelled, heard, touched, and felt. Our experiences reflect what the world has exposed to us. Many of those experiences hinge on what others thought and experienced long before us: Our thoughts are a combination of the views of generations past; our words are a pastiche of ourselves and others and the life experiences of many people at once. As a result, we can't model information transmission as a simple path from *A* to *B*. Rather, most transmissions will be a complex meandering journey from *A* to *B* to *C* to *D* to *E* with U-turns and curves along the way.

This complexity inhibits ex ante clarity for the police because they will necessarily collect information at the end of its dissemination, whereas judgments as to whether and when privacy is likely must be made prospectively.

---

106. *See, e.g.*, Solove, *supra* note 64, at 1083 (criticizing the third-party doctrine, but not proposing a clear alternative to it).

107. *See generally* Kerr, *supra* note 100, at 503.

108. *See id.* at 508–12.

109. *Id.*

From the perspective of the individual sending out information, who is curious about whether he will maintain his rights, he will assess whether the information recipient appears trustworthy. He might ask whether the recipient has a privacy policy, and might ask whether he has failed to maintain privacy in the past to predict what may happen in the future. But criminal investigators do not have this luxury. They must roll the tape backwards, starting with the present and trying to reconstruct the past. The determination of whether an expectation of privacy is reasonable in a probabilistic sense is highly contextual, and the context will be dramatically different at various transfer points in the history of information. As a result, the Fourth Amendment rules that the police must apply ex ante must hinge on details of the history of information that they cannot know ex ante and may be unable to reconstruct at all.

A simple example demonstrates the problem. Imagine that a federal prosecutor is a regular reader of CorruptionWatch.com, a blog about public corruption crimes. One day he visits the blog and finds an anonymous comment left by an unidentified reader: "I heard that Senator Smith was seen in public today depositing a $50,000 check from Jack Abramoff into Senator Smith's personal account at Ames Bank. Did Abramoff bribe him? Does anyone know? Email me at SenatorSmithsSecrets@gmail.com."

The prosecutor is curious about what the commenter knows, and he wants to subpoena the author of the comment. But what Fourth Amendment rule would govern such a subpoena? Under the third-party doctrine, the rule is the traditional one for issuing subpoenas. The history of the information is irrelevant to the legal rule that must be followed. But imagine a world in which the current third-party doctrine is replaced with a probabilistic model. Suddenly the Fourth Amendment rule is unclear. We do not know whether the subpoena will implicate Senator Smith's reasonable expectation of privacy because we don't know who the commenter is or how he came to know what he knows.

Consider five possibilities. In the first, the comment author is the bank teller who served Senator Smith and helped him deposit the check. In the second, the author is a fellow Ames Bank customer in line behind Senator Smith who overheard Senator Smith loudly announcing that he was there to deposit a $50,000 check from Jack Abramoff. In the third, the author is a bank robber who broke into the bank and looked through Senator Smith's files. In the fourth, the author is Jack Abramoff, who wants to get Senator Smith in trouble so he can negotiate a better deal with the feds. In the fifth, the author is Senator Smith himself, who was just curious to see if anyone would believe the story if he posted it online anonymously. In which of these cases would the subpoena violate Senator Smith's reasonable expectation of privacy under a probabilistic approach—that is, where a reasonable expectation of privacy is based on a probabilistic assessment of whether Senator Smith would reasonably expect his conduct to be widely disseminated? Perhaps the answer is that the first and third violate a reasonable expectation of privacy, the second and fifth do not, and the fourth depends on the details of the relationship between Smith and Abramoff. But how can

But commenter
knows has expectation
of privacy?

how is that different?

question is just how
weight?

Still need subpoena for Gmail
But not for letter on desk

the police know this? They need to know what they will learn before they can know ex post if their conduct violated the Fourth Amendment.

And this is just the tip of the iceberg. Matters get much more complicated if the Fourth Amendment recognizes information history past the immediate question of the most recent "hop" back from its final resting point. For example, Joe might tell a secret to Jane, who might share it with Ben, who might write it in his diary that is stolen by Sarah, who might post it on a blog that is read by Earl, who might tell it in confidence to a government informant. Now ask the question: did the informant's learning the information violate anyone's reasonable expectation of privacy? We need to look past Earl, as we also need to answer the question for Sarah, Ben, Jane, and Joe. And for that matter, we need to know how Joe knew the secret in the first place; we need to trace the information to the very moment it appeared that someone's reasonable expectation of privacy might be violated. And of course all of that information must be known before the information is even acquired; somehow the police must know the detailed information history of information they have not yet seen. Under the third-party doctrine, these extremely difficult questions no longer need be asked. Information history becomes irrelevant.

C. *Ex Ante Clarity with a Policy-Based Alternative*

A second alternative to the existing third-party doctrine would be what I have termed a policy-based approach.[110] Under this approach, a reasonable expectation of privacy exists when, as a matter of policy, it is better for a particular practice to be regulated by a warrant requirement than for it to be unregulated by the Fourth Amendment.[111] When courts apply a policy model, they categorize the case before them and decide whether a reasonable expectation of privacy should extend as a matter of policy to that category of facts. A policy approach clearly can lead to greater clarity than the probabilistic method, as it provides a way for courts to generate rules that apply to categories of cases. However, generating clear Fourth Amendment rules based purely on policy considerations turns out to be relatively difficult.

In my view, there are two major difficulties with using policy-based rules to generate clear rules over third-party information. The first problem is that there are hundreds of potentially distinct applications of the third-party doctrine, and courts would need to apply the policy model to each of them to determine whether the information should be protected. The third-party doctrine is one size fits all; there is no need for case-by-case policy balancing. But if courts try to engage in policy balancing for each type of record, they will be forced to resolve how the balancing applies to a very wide range of cases. For example, many critics may want to overrule *Miller*, the case involving bank records, or *Smith*, the case involving pen registers.

110. *See id.* at 519–22.

111. *Id.*

But what about Fourth Amendment rules for credit card records? Electricity records? Gas meter records? Telephone records? Internet records? IP addresses? Book store records? Clothing store records? Record store records? iTunes accounts? Undercover agents wearing wires? Undercover agents not wearing wires? Until each of these questions was settled by the courts, agents would have no way of knowing how the law governed access to such information.

Second, because many applications of the third-party doctrine involve developing technologies, the outcome of a policy-based determination of how the Fourth Amendment should apply to third-party information can change over time.[112] Consider how the Fourth Amendment could apply to so-called trap-and-trace information: information obtained through the government's collection of incoming telephone numbers for a particular telephone account.[113] Until the spread of "caller ID" services, most individuals presumably thought of caller ID information as private; today, on the other hand, the disclosure of the incoming telephone number is simply a standard part of placing a telephone call. The changing social meaning of trap-and-trace information can create uncertainty for police investigators. If courts change the Fourth Amendment answer as the social meaning changes, how can police officers know when that will occur?

These challenges may not be insurmountable. Perhaps courts could hammer out rules for applying the Fourth Amendment to each of these types of records. Perhaps the answers would change only gradually and courts could keep up reasonably well. But at the same time, it is important to see that creating these doctrines would in fact pose a major practical challenge. All but a few critics have ignored this. As far as I know, only Professor Slobogin has attempted to offer a comprehensive alternative to the third-party doctrine.[114] Professor Henderson has offered a nine-factor totality-of-the-circumstances test,[115] but the factors and their application are so vague that they offer no clarity ex ante.[116] If critics want to replace the third-party doctrine with an alternative, they should be clearer about what that alternative would be and how it would apply in the wide range of cases courts regularly confront.

---

112. I have developed this argument in greater depth in Kerr, *supra* note 92, at 871–75.

113. *See generally* 18 U.S.C. § 3127(4) (Supp. V 2005) (defining trap-and-trace devices for purposes of the Pen Register statute).

114. SLOBOGIN, *supra* note 5, at 179–96. I critique Professor Slobogin's proposal elsewhere in this Volume of the *Michigan Law Review*. Orin S. Kerr, *Do We Need a New Fourth Amendment?*, 107 MICH. L. REV. (forthcoming April 2009) (reviewing SLOBOGIN, *supra* note 5).

115. Henderson, *supra* note 5.

116. Professor Henderson's nine factors are (1) the purpose of the disclosure, (2) the personal nature of the information, (3) the amount of information, (4) the expectations of the disclosing party, (5) the understanding of the third party, (6) positive law guarantees of confidentiality, (7) government need, (8) personal recollections, and (9) changing social norms and technologies. *Id.* at 975.

IV. Responding to Criticisms of the Third-Party Doctrine

The third-party doctrine is no panacea. Section I.B explained that the many critics of the third-party doctrine have made two primary arguments against it, one doctrinal and the other functional. The doctrinal claim is that the Justices are wrong when they contend that a person does not retain a reasonable expectation of privacy. According to these critics, people will often reasonably expect privacy in their third-party information.[117] The Justices misunderstand privacy because they fail to realize the difference between exposure to one person and exposure to the public.[118] The second argument, the functional claim, is that the third-party doctrine is incorrect because it gives the government too much power. It gives the police carte blanche power to access business records, and the prospect of abuses makes such powers inconsistent with a free society and therefore with the Fourth Amendment.[119]

This Part argues that while both criticisms have some force, both considerably overstate the case and ignore important counterarguments. First, the doctrinal argument ends up being mostly about form rather than substance. Although critics are right that the Court's applications of the *Katz* test to undercover agents and third-party records are awkward, that is largely because the third-party cases are better understood as consent cases. Disclosure to third parties eliminates protection because it implies consent. When the cases are understood as a subset of consent law rather than as applications of the reasonable expectation of privacy test, the doctrinal criticism ends up being much narrower than critics suggest.

The functional arguments about government power correctly note that the third-party doctrine permits invasive practices that could be abused by overzealous and even corrupt officials. However, they overlook the legal system's many substitutes for Fourth Amendment protection. In the absence of Fourth Amendment regulation, all three branches have created limits on the use of secret agents and access to business records that address many of the critics' concerns. Common law privileges, entrapment law, the *Massiah* doctrine, First Amendment doctrine, and statutory privacy protections have been designed specifically to address concerns of police harassment in the use of third parties.[120] Although the critics are justified in fearing abuses, they have wrongly viewed the Fourth Amendment in isolation. The full panoply of legal responses to third-party records and secret agents reveals that Fourth Amendment protection is only one among many legal tools to address these concerns. As a result, the functional argument against the third-party doctrine is significantly weaker than the critics imagine.

---

117. *See supra* Section I.B.1.

118. *See supra* Section I.B.1.

119. *See supra* Section I.B.2.

120. All of these doctrines are discussed *infra* Part IV.

A. *The Third-Party Doctrine as a Consent Doctrine*

First consider the doctrinal criticism that the Supreme Court is incorrect when it says that individuals cannot retain a reasonable expectation of privacy in third-party information. In my view, the doctrinal critics are partially right. The Supreme Court's applications of the reasonable expectation of privacy test to third-party information have been awkward and unconvincing. But the reason is that the third-party doctrine is better understood as a form of consent rather than as an application of *Katz*. Third-party disclosure eliminates privacy because the target voluntarily consents to the disclosure, not because the target's use of a third party waives a reasonable expectation of privacy. The difference is subtle but conceptually important, and I think it reveals that the doctrinal critique is a significantly narrower claim than critics believe.[121]

The notion of treating the third-party doctrine as a consent problem arguably goes back to the briefing of *Hoffa v. United States*[122] in 1966, the year before *Katz*. Hoffa's merits brief before the Supreme Court argued that the deception by a secret agent, Partin, had vitiated Hoffa's consent. Hoffa had been tricked, and his consent to let Partin listen in was no longer legally valid: "The Government's deception in hiding the informer under his [union] roles . . . prevented any intelligent and understanding waiver of Petitioner Hoffa's Fourth Amendment rights."[123] The government's brief responded that Partin's motive had not invalidated the consent: Hoffa had knowingly and intentionally admitted Partin into his private spaces and had shared evidence of his crime with Partin.[124] Having consented to Partin's presence, Hoffa had waived any Fourth Amendment rights.[125]

The Supreme Court should have accepted this consent-based formulation of the third-party doctrine. The parties in *Hoffa* accurately identified the issue raised by the third-party doctrine: When does a person's choice to disclose information to a third party constitute consent to a search? Further, the result in *Hoffa* sided with the correct answer: So long as a person knows that they are disclosing information to a third party, their choice to do so is voluntary and the consent valid. The fact that a person turns out to be an undercover agent should be irrelevant to whether the consent is valid, as that representation is merely fraud in the inducement rather than fraud in the factum.[126] A person who knowingly discloses information to a third party

---

121. A second response is that many critics wrongly assume that a probabilistic model of the "reasonable expectation of privacy" test is the only correct one. This is not true, as I have argued elsewhere. *See* Kerr, *supra* note 100.

122. 385 U.S. 293 (1966).

123. Brief for Petitioners at 35–36, Hoffa v. United States, 385 U.S. 293 (1966) (Nos. 32, 33, 34, 35).

124. Brief for the United States at 125–26, *Hoffa*, 385 U.S. 293 (Nos. 32, 33, 34, 35).

125. *Id.*

126. *See* ROLLIN M. PERKINS & RONALD N. BOYCE, CRIMINAL LAW 1079 (3d ed. 1982). Perkins and Boyce note:

may be tricked as to what the third party will do with the information. But trickery as to motive or design does not vitiate consent.[127]

How did the Supreme Court get off course? The critical juncture was *United States v. White*,[128] the first third-party case to follow *Katz*. In that case, Justice White tried to fit the third-party doctrine into the Court's post-*Katz* Fourth Amendment, but he simply chose the wrong doctrinal prong. Instead of grounding the doctrine in consent principles, he reasoned that use of a secret agent did not violate a reasonable expectation of privacy. The difference between the two is subtle: If government conduct does not violate a reasonable expectation of privacy, it is not a search,[129] whereas if it violates a reasonable expectation of privacy pursuant to consent, it is a search but one that is constitutionally reasonable.[130] At the same time, the two cover conceptually distinct ground. The reasonable expectation of privacy inquiry focuses on whether the government conduct intruded into constitutionally protected areas,[131] whereas consent asks whether it did so with permission.[132]

Later cases adopted Justice White's framework uncritically, establishing the third-party doctrine as an application of the *Katz* test.[133] But this doctrinal home never fit. Sharing space with others does not eliminate Fourth Amendment protection: The police need a warrant to enter a shared home just as much as they do an unshared one.[134] If two people share a home or an office, they still retain a constitutional reasonable expectation of privacy there.[135] Sharing space provides the co-occupant with common authority to permit their consent,[136] but it does not relinquish all Fourth Amendment protection. Similarly, the third-party doctrine is best understood as a shared space doctrine. By knowingly disclosing information to a third party, an individual consents to another person having control over it. The doctrine

---

> The general rule is that if deception causes a misunderstanding as to the fact itself (fraud in the *factum*) there is no legally-recognized consent because what happened is not that for which consent was given; whereas consent induced by fraud is as effective as any other consent . . . if the deception relates not to the thing done but merely to some collateral matter (fraud in the inducement).

Id.

127. *See id.* at 1075–84.

128. 401 U.S. 745 (1971).

129. Smith v. Maryland, 442 U.S. 735, 740 (1979).

130. *See* Georgia v. Randolph, 547 U.S. 103, 114–15 (2006).

131. *See* Kyllo v. United States, 533 U.S. 27, 31 (2001) (citing Silverman v. United States, 365 U.S. 505, 510–12 (1961)).

132. *See Randolph*, 547 U.S. at 114–15.

133. *See supra* Section II.B.

134. *See* Mancusi v. DeForte, 392 U.S. 364 (1968) (holding that a person retains a reasonable expectation of privacy in a shared office).

135. *Id.* at 369–70.

136. *See* United States v. Matlock, 415 U.S. 164, 171 n.7 (1974) (noting that "common authority" over spaces or property gives co-inhabitants the right to permit inspections of their own accord).

sounds in consent, not reasonable expectations of privacy, and it fits within the rest of Fourth Amendment law when so understood.[137]

Importantly, while this point narrows the scope of the doctrinal critique, it does not eliminate it entirely. In particular, it does not address cases like *Miller* where the government forces a third party to disclose records after the suspect voluntarily discloses the record to the third party. The suspect has consented to third-party access in such cases, but neither he nor the third party has consented to the subsequent government access. This is a fair point. But I think it is also a narrow one, as at this point the third-party doctrine becomes merely an application of the general rule that the Fourth Amendment does not regulate subpoenas to testify.[138] Any witness can be compelled to testify about what he knows and what he has seen without Fourth Amendment oversight,[139] and the third-party doctrine merely refrains from carving out an exception to this rule for confidential disclosures to third parties.

B. *Alternatives to Fourth Amendment Protections to Prevent Harassment—The Case of Secret Agents*

The second major criticism of the third-party doctrine is that it gives the police too much power.[140] The doctrine permits government officials to send in spies, use informants, get bank records, record numbers dialed, and obtain billing records of entirely innocent people without any cause or court-order requirement. According to critics, giving the government this much power is inconsistent with a free and open society; the risk of misuse and harassment is too great.[141]

The problem with this argument is that it assumes the Fourth Amendment is the only game in town. In truth, a wide range of tools exists for addressing police harassment of third-party information outside the Fourth Amendment. These tools substitute for Fourth Amendment protection, prohibiting or limiting access to third-party evidence in specific settings that may be subject to abuse. In the case of secret agents, the legal system uses entrapment law, the *Massiah* doctrine, the First Amendment, and internal regulations to limit the government's use of secret agents.

To be clear, there is considerable room for debate on the sufficiency of these substitutes for Fourth Amendment protection. The warrant requirement is strong medicine, and some of the nonconstitutional substitutes are modest by comparison. Most are designed to deter bad faith investigations

---

137. Notably, Professor Colb has argued that the Supreme Court's "knowing exposure" cases should be reanalyzed under consent principles. *See* Colb, *supra* note 67, at 123. However, Professor Colb does not focus this insight on the third-party doctrine cases specifically. Further, she does not suggest that the consent doctrine might help justify the existing third-party doctrine cases.

138. United States v. Dionisio, 410 U.S. 1, 9 (1973).

139. *See id.* at 10.

140. *See supra* Section II.B.2.

141. *See supra* Section II.B.2.

rather than to keep the government from accessing information altogether, and observers may disagree on which doctrines succeed or fail. But this should not obscure the deeper point: Fourth Amendment protection is only one tool among several for addressing police harassment. The absence of Fourth Amendment protection does not mean police practices go unregulated. Rather, it means a shift from regulation through a probable cause warrant requirement to regulation through privileges, entrapment doctrine, the Sixth Amendment, the First Amendment, statutes, and other forms of third-party protection.

In short, critics suffer from constitutional myopia. While they focus on the failure of the Fourth Amendment to stop government harassment and limit the power of the state, they tend to overlook the substitutes that already address the same concerns through other means. Properly conceived, the choice is not between Fourth Amendment protection and none, but rather between regulation by a diverse set of doctrines or that diverse set of doctrines plus the added protection of the Fourth Amendment. As a result, critics overstate the degree of government power that the third-party doctrine authorizes.

We can begin by considering how the law outside the Fourth Amendment tries to regulate secret agents. Although the Fourth Amendment does not regulate the use of secret agents,[142] four other bodies of law help fill in the gap: entrapment law; the *Massiah* doctrine; the First Amendment; and internal agency regulations. All four bodies of law deter abuses of secret agents. They prohibit the use of secret agents in some cases and ensure that they are used only in relatively limited ways in others.

1. *Entrapment Law*

Entrapment law provides the first substitute for Fourth Amendment regulation of secret agents. Entrapment is a judicially created doctrine,[143] recognized by statute in some states,[144] that regulates how the police use secret agents. Although there are several forms of entrapment law, the overarching purpose of the doctrine is to impose a requirement of reasonable police practices in the use of secret agents. If the police target an innocent person, one who has shown no predisposition to commit an offense, the undercover officer cannot induce the target into committing a crime.[145] "Inducement" occurs when the undercover agent pressures the suspect to commit the offense, either by badgering him or encouraging him to commit the offense in a way calculated to persuade the suspect based on his personality.[146] The remedy is an affirmative defense to prosecution rather

142. *See supra* Section I.A.1.

143. *See* 2 WAYNE LAFAVE ET AL., CRIMINAL PROCEDURE § 5.1(b) (3d ed. 2007).

144. *Id.*

145. *See, e.g.*, Sherman v. United States, 356 U.S. 369 (1958).

146. United States v. Gendron, 18 F.3d 955, 961–62 (1st Cir. 1994). Examples listed by then-Judge Breyer in *Gendron* include cases in which the secret agent (1) used intimidation and threats

than the suppression of evidence, meaning that the reasonableness of the government's conduct is evaluated by a jury instead of a judge.

Entrapment law does directly what critics of the third-party doctrine want done indirectly: It regulates abusive law enforcement practices targeting innocent defendants who are not actually suspected of a crime. The basic concern animating entrapment law is much the same as the concern animating the functional critique of the third-party doctrine: "The crucial question . . . is whether the police conduct revealed in the particular case falls below standards . . . for the proper use of governmental power."[147] But instead of regulating the use of undercover investigations ex ante, entrapment law prohibits their abuse in practice ex post. Instead of regulating *when* secret agents can be used, it regulates *how* they are used. The principles of entrapment law monitor the government's conduct, giving the jury a basis to acquit a defendant if the government implants the idea of the crime in the suspect's mind.

If the Fourth Amendment regulated secret agents, entrapment law would not be necessary. In such a world, the government would only use secret agents when it had probable cause that the suspect would reveal evidence of a crime, and that evidence would prove predisposition to defeat an entrapment defense.[148] Entrapment law has evolved as a byproduct of the third-party doctrine; it was created by the courts to fill in gaps that the third-party doctrine leaves open.

2. *The* Massiah *Doctrine*

The second substitute for Fourth Amendment regulation of secret agents is the *Massiah* doctrine. In *Massiah v. United States*,[149] the Supreme Court held that an agent of the government cannot question a person who has been charged with a crime.[150] Massiah had been indicted on drug charges, retained a lawyer, and was released on bail. Massiah later met with his co-conspirator Colson, and discussed his drug crimes with Colson when in Colson's car.[151] Unbeknownst to Massiah, Colson had flipped and was acting

---

against a defendant's family; (2) called every day, began threatening the defendant, and was belligerent; (3) engaged in forceful solicitation and dogged insistence until defendant capitulated; (4) played upon defendant's sympathy for informant's common narcotics experience and withdrawal symptoms; (5) played upon sentiment of one former war buddy for another to get liquor (during prohibition); (6) used repeated suggestions which succeeded only when defendant had lost his job and needed money for his family's food and rent; and (7) told defendant that she (the agent) was suicidal and in desperate need of money.

147. *Sherman*, 356 U.S. at 382 (Frankfurter, J., concurring).

148. If the government cannot use a secret agent without probable cause to believe that the agent will uncover evidence of crime from the target, presumably that means that the government has prior evidence that the target is predisposed to engage in criminal activity.

149. 377 U.S. 201 (1964).

150. *Id.* at 207 ("[W]e hold . . . that the defendant's own incriminating statements, obtained by federal agents under the circumstances here disclosed, could not constitutionally be used by the prosecution as evidence against *him* at his trial.").

151. *Id.* at 202–03.

as an informant for the government. Agents had bugged Colson's car and directed Colson to discuss his crimes with Massiah. An agent named Murphy listened in on the conversation and heard Massiah's incriminating statements.[152] At trial, Murphy testified about what he heard over Massiah's objection. When the *Massiah* case reached the Supreme Court, Massiah argued that the secret surveillance violated the Fourth, Fifth, and Sixth Amendments.[153]

The Supreme Court ruled that this use of a secret agent had violated Massiah's Sixth Amendment rights.[154] First, the Court held for the first time that a person who has been indicted and is represented by counsel has a right not to be questioned by an agent of the state outside the presence of his attorney.[155] Second, the Court held that the fact that the "agent" was a confidential informant made no difference.[156] Indeed, the fact that Massiah had been questioned by a confidential informant instead of a uniformed police officer made the violation of his rights more egregious: " 'Massiah was more seriously imposed upon . . . because he did not even know that he was under interrogation by a government agent.' "[157]

The *Massiah* doctrine regulates the use of third parties at the opposite end of the investigative process from entrapment law. Entrapment law concerns itself with how the government approaches suspects on the front end of investigations: The government cannot use third parties to create crime that otherwise would not have occurred. The *Massiah* doctrine concerns itself with how the government approaches suspects near the end of the process: Under *Massiah*, the government cannot use secret agents to obtain information about the crime from a target who has already been charged. While the Fourth Amendment permits the use of secret agents generally, the *Massiah* doctrine carves out one potentially abusive consequence of this rule by prohibiting the practice after a person has been represented by counsel.[158]

3. *The First Amendment*

The First Amendment may also impose restrictions on the use of undercover operations. Generally speaking, the First Amendment is implicated when government investigators infiltrate groups that engage in First

---

152. *Id.*

153. *Id.* at 203–04.

154. *Id.* at 205–06.

155. *Id.* at 207.

156. *Id.* at 206.

157. *Id.* at 206 (alteration in original) (quoting United States v. Massiah, 307 F.2d 62, 72–73 (2d Cir. 1962) (Hays, J., dissenting)).

158. This is true so long as the secret agent asks about the crime charged; the Sixth Amendment does not prohibit inquiries about unrelated crimes. *See* Texas v. Cobb, 532 U.S. 162, 172–74 (2001).

Amendment activities without a good faith reason for doing so.[159] This good faith test addresses one result that critics of the third-party doctrine fear the Fourth Amendment allows: investigations that are designed to target individuals exercising their First Amendment rights.

United States v. Mayer[160] offers a recent example. In *Mayer*, an undercover FBI agent infiltrated the North American Man/Boy Love Association ("NAMBLA"): a group that claimed to be " 'a political, civil rights and educational organization' " opposed to age-of-consent laws.[161] After becoming an active member of the group, the undercover agent encountered several discussions of illegal activity. One group member named Mayer expressed in frustration that "NAMBLA kept up pretenses of trying to change society when in fact its members only wanted to travel to meet boys."[162] The undercover agent then arranged a trip for NAMBLA members to meet boys, and Mayer signed up to go on the trip. When Mayer was arrested for traveling in interstate commerce with intent to engage in illegal sexual activities, he claimed that the government's infiltration of NAMBLA violated the First Amendment.

The Ninth Circuit explained that use of a secret agent to infiltrate a First Amendment-related group is permitted only when it is "justified by a legitimate law enforcement purpose that outweighs any harm to First Amendment interests."[163] The court found that this requirement was satisfied, under the circumstances, by reports of illegal activity the police had received relating to members of the NAMBLA group: Given the facts, the government's "interests in pursuing legitimate law enforcement objectives outweighed any harm to First Amendment interests."[164] Had the undercover investigation lacked a legitimate law enforcement purpose, or been undertaken to abridge First Amendment freedoms, then the investigation would have violated the First Amendment even though it did not implicate the Fourth Amendment.

4. *Internal Agency Regulations*

Internal agency regulations provide a fourth tool for limiting the use of secret agents. At the federal level, for example, the Justice Department has promulgated the *Attorney General's Guidelines on Federal Bureau of*

---

159. *Cf.* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958) (invalidating a production order for members of the local NAACP on the ground "that the production order, in the respects here drawn in question, must be regarded as entailing the likelihood of a substantial restraint upon the exercise by petitioner's members of their right to freedom of association").

160. 503 F.3d 740 (9th Cir. 2007).

161. *Id.* at 745.

162. *Id.* at 747.

163. *Id.* at 753.

164. *Id.*

Investigation Undercover Operations.[165] The *Guidelines* require the Special Agent in Charge of each FBI office to preapprove every FBI undercover investigation based on a written determination, supported by specific facts, that the proposed operation will be effective and will be conducted in a minimally intrusive way.[166] Undercover operations can be approved for up to six months and renewed for one more six month period.[167] They ordinarily cannot involve expenditures of more than $50,000.[168]

The *Guidelines* have special rules for particularly sensitive undercover investigations. FBI Headquarters must preapprove investigations of political organizations, religious groups, the news media, or public officials.[169] A Criminal Undercover Operations Review Committee consisting of FBI and DOJ officials meets to review these applications, and it must reach a consensus as to the appropriateness of each application.[170] If the Committee recommends approval of an application, it must include a statement as to why the operation merits approval in light of the sensitive nature of such investigations.[171] The Justice Department has promulgated roughly analogous guidelines for the use of confidential informants.[172] Like the limitations imposed by entrapment law, *Massiah*, and the First Amendment, these agency rules attempt to foreclose use of secret agents in bad faith or abusive contexts.

C. *Substitutes for Fourth Amendment Protection in Business Record Cases*

Just as several legal tools regulate the use of secret agents, there are many substitutes for Fourth Amendment protection of business records. The three legal tools that predominate are statutory protections, common law privileges, and rights of the third parties themselves. These doctrines regulate the government's access to business records outside the Fourth Amendment, deterring the kinds of abuses that critics fear may come to pass under the third-party doctrine. In some instances these tools require court orders or special cause to access third-party records; in other instances they block access to third-party records altogether. Taken together, these doctrines limit considerably the threat that the third-party doctrine poses to civil liberties. Once again, reasonable minds can differ about whether they do

like movie rentals?

165. JOHN ASHCROFT, ATT'Y GEN., THE ATTORNEY GENERAL'S GUIDELINES ON FEDERAL BUREAU OF INVESTIGATION UNDERCOVER OPERATIONS (2002), *available at* http://www.usdoj.gov/olp/fbiundercover.pdf.

166. *Id.* at 3–4.

167. *Id.* at 4.

168. *Id.*

169. *Id.* at 6.

170. *Id.* at 8.

171. *Id.* at 8.

172. *See* Department of Justice Guidelines Regarding the Use of Confidential Informants (Jan. 8, 2001), http://www.usdoj.gov/ag/readingroom/ciguidelines.htm.

enough in specific cases. But these doctrines help address the threat to privacy and individual rights that critics observe when viewing the third-party doctrine in isolation.

1. *Statutory Protections*

The most obvious alternatives to constitutional regulation for access to business records are statutory protections. Statutory privacy laws can impose a court-order requirement on government evidence collection even if the Fourth Amendment does not. The result can deter harassment of the innocent by introducing judicial supervision over investigations and effectively requiring officials to prove a legitimate government interest in the information sought.

For example, in response to *Smith*,[173] Congress enacted the Pen Register and Trap and Trace Devices Statute, codified at 18 U.S.C. 3121–3127.[174] *Smith* held that the Fourth Amendment does not limit the use of pen register devices to determine the numbers dialed from a telephone.[175] However, the Pen Register statute makes it a crime to install a pen register without a court order, subject to some exceptions. Obtaining a court order is quite easy under the statute: Investigators need only certify that "the information likely to be obtained . . . is relevant to an ongoing criminal investigation."[176] But this still imposes a good faith test: The law requires an actual ongoing investigation and a good faith belief in the likelihood that evidence to be obtained is relevant to that investigation.

Similarly, in response to *Miller*,[177] Congress enacted the Right to Financial Privacy Act ("RFPA").[178] RFPA responds to *Miller* by limiting government access to "the information contained in the financial records of any customer from a financial institution"[179] where the Fourth Amendment, thanks to *Miller*, does not. Under RFPA, the government can obtain such financial records with a subpoena only if the government has "reason to believe that the records sought are relevant to a legitimate law enforcement inquiry" and the government first provides the suspect with prior notice of the planned action that gives him an opportunity to move to quash the subpoena.[180]

In some cases, statutory protections for third-party records have been enacted even absent court decisions. For example, the Health Insurance

---

173. Smith v. Maryland, 442 U.S. 735 (1979).

174. 18 U.S.C. §§ 3121–3127 (2000 & Supp. V 2005).

175. *Smith*, 442 U.S. at 743.

176. 18 U.S.C. § 3123(a) (2000).

177. United States v. Miller, 425 U.S. 435 (1976).

178. 12 U.S.C. §§ 3401–3422 (2006).

179. 12 U.S.C. § 3402.

180. 12 U.S.C. § 3407.

Portability and Accountability Act ("HIPAA") protects medical records;[181] the Privacy Protection Act restricts government access to third-party records held by newsgathering organizations;[182] the Video Privacy Protection Act provides special privacy protections for video rental records;[183] the Stored Communications Act restricts access to email account records;[184] and the Cable Act restricts access to cable account records.[185] These laws all impose statutory restrictions on access to records that the third-party doctrine leaves unprotected under the Fourth Amendment.

In many (but not all) of these cases, the statutory privacy laws provide less protection than would the analogous Fourth Amendment standard of a probable cause warrant.[186] But that is a good thing rather than a bad one. The fact that standards are low prevents the end-run around the balance of Fourth Amendment rules that outsourcing can permit. At the same time, the standards are substantial enough to make it quite unlikely that the police would use the investigative powers solely to harass innocent suspects. In the case of financial records, a suspect could move to quash the subpoena, which would provide a court audience to hear his complaint of government overreaching. And in the case of pen registers, the government must first go to a judge and seek an order, certifying under oath that an ongoing investigation exists and that the information collected is likely to be relevant. These intermediate standards deter wrongful abuse while permitting legitimate investigations. They strike a middle ground not possible under the Fourth Amendment.

2. *Common Law Privileges*

Common law privileges provide a second tool for regulating access to business records. When a suspect has a privileged relationship with a third party, the third-party records cannot be accessed by the government. As a practical matter, the privilege trumps the third-party doctrine. It forces the government to take a hands-off approach to what otherwise might be very embarrassing information or important evidence of criminal activity.

The most obvious example of a privilege that trumps the third-party doctrine is the attorney-client privilege. In the federal system, privileges are recognized by Federal Rule of Evidence 501: "[T]he privilege of a witness [or] person . . . shall be governed by the principles of the common law as they may be interpreted by the courts of the United States in the light of reason and

---

181. 45 C.F.R. § 164.512(f)(1)(ii)(A) (2007) (permitting disclosure of medical records pursuant to "[a] court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer").

182. 42 U.S.C. § 2000aa (2000).

183. 18 U.S.C. § 2710.

184. 18 U.S.C. § 2703(c) (Supp. V 2005).

185. 47 U.S.C. § 551(h).

186. The major exception is the Cable Act, which allows disclosure of cable records only in very narrow circumstances. *Id.*

experience."[187] Under the attorney-client privilege, "[c]onfidential disclosures by a client to an attorney made in order to obtain legal assistance are privileged."[188] This rule encourages "full and frank communication between attorneys and their clients and thereby promote[s] broader public interests in the observance of law and administration of justice."[189] Evidence collected in violation of the privilege must be suppressed.[190]

The attorney-client privilege is not the only privilege recognized by federal courts. The Supreme Court recognized a psychotherapist-patient privilege in *Jaffee v. Redmond*.[191] And although the Supreme Court has not addressed the issue, lower federal courts have generally recognized a priest-penitent privilege.[192] All of these privileges effectively trump the third-party doctrine in specific settings where outsourcing of crime is particularly unlikely or there are powerful competing needs beyond evidence collection. A suspect is unlikely to use his attorney, his priest, or his psychotherapist to facilitate his crimes, and professional lawyers, clergymen, and psychologists are unlikely to be willing to participate in advancing a client's criminal scheme. At the same time, the privilege is needed to permit individuals to benefit from the advice of their lawyers, priests, and therapists. In these settings, the privilege effectively ameliorates the potential threat of government abuses raised by the third-party doctrine.

3. *The Rights of Third Parties*

The final tool for regulating government access to third-party business records is through the rights of the third parties themselves. In some cases, third parties in possession of business records may be willing to cooperate with the police. In many contexts, however, third parties may want to assert the rights of their customers. Protecting customer privacy is good for business, and third-party record holders often have a considerable incentive to keep the government at bay. An early illustration is the famous amicus brief that the telephone companies filed in the Supreme Court's first wiretapping case, *Olmstead v. United States*.[193] The phone companies urged the Supreme Court to rule that the government could not wiretap telephone lines.[194] Such a rule made good business sense for the telephone companies: It would both encourage customers to use the telephone and keep the government from interfering with their networks.

---

187. FED. R. EVID. 501.

188. Fisher v. United States, 425 U.S. 391, 403 (1976).

189. Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

190. *See* United States v. White, 887 F.2d 267, 275 (D.C. Cir. 1989).

191. 518 U.S. 1, 15 (1996).

192. Cox v. Miller, 296 F.3d 89, 102 n.6 (2d Cir. 2002) (citing cases).

193. 277 U.S. 438 (1928).

194. Brief for Pacific Telephone & Telegraph Co. et al. as Amici Curiae Supporting Petitioners, Olmstead v. United States, 277 U.S. 438 (1928) (Nos. 493, 532, 533).

A more recent example demonstrates how modern third-party providers can assert the rights of customers despite the third-party doctrine. In 2006, in the midst of civil litigation on the constitutionality of the Child Online Protection Act, the Department of Justice issued subpoenas ordering several search engine companies to disclose user queries for a two-month window.[195] DOJ claimed to need this information to determine how internet users used search engines to obtain pornography, which could then help determine the effectiveness of Internet filters.[196] When Google objected to the subpoenas, DOJ agreed to a narrower subpoena seeking a million random queries and all of the searches for a one-week window.[197] Google then continued to object, and moved to quash the subpoenas on the grounds that they sought information that was irrelevant and that production would be an undue burden. Google made the case somewhat creatively, arguing that "potential for loss of user trust" was a "burden" on Google that should require the subpoenas to be quashed.[198]

District Court Judge James Ware used these legal principles to fashion a narrow subpoena that protected the privacy interests of Google users. As modified by Judge Ware, the subpoena required Google to create a database that offered a random selection of 50,000 website addresses that could be accessed through the Google search engine.[199] Judge Ware raised sua sponte the question of the privacy interests of Google users—not Fourth Amendment privacy interests, to be clear, but more general privacy interests in the disclosure of information users had sent to Google in their queries.[200] Judge Ware noted that search queries could contain personal information, citing vanity queries or queries for sexually explicit information as examples of queries that raise privacy concerns.[201] And he fashioned a subpoena that would allow the government to conduct a study on Google's results without resulting in the disclosure of third-party queries made by users.

In a number of cases, third parties have also successfully asserted First Amendment interests of users in response to subpoenas allowed under the Fourth Amendment. For example, in *Doe v. Gonzales*,[202] a Connecticut Internet Service Provider successfully argued that the First Amendment afforded it a right to disclose service of a National Security Letter for third-party record information. In another recent subpoena case, a magistrate judge ruled that a grand jury subpoena for third-party records of book purchases violated the First Amendment by triggering a likely chilling effect on

---

195. *See* Declan McCullagh, *FAQ: What does the Google subpoena mean?*, CNET NEWS, Jan. 20, 2006, http://news.cnet.com/2100-1029_3-6029042.html.

196. *Id.*

197. *Id.*

198. Gonzales v. Google, Inc., 234 F.R.D. 674, 683 (N.D. Cal. 2006).

199. *Id.* at 688.

200. *Id.* at 687.

201. *Id.*

202. 500 F. Supp. 2d 379 (S.D.N.Y. 2007).

purchasing.[203] In addition, several courts have imposed First Amendment restrictions on subpoenas for third-party records in the civil context.[204]

I do not argue that third-party business record holders will always assert these arguments in defense of their customers. Indeed, recent headlines[205] about how telecommunications providers voluntarily assisted the NSA in collecting third-party records (quite possibly in violation of statutory privacy laws)[206] reaffirm that sometimes third-party providers will cooperate eagerly with the government. But the point is broader. Third-party business record holders can recognize the advantages of fighting for the privacy rights of their customers even absent Fourth Amendment protection. The prospect of resistance from the legal teams of third-party record holders often creates a substantial deterrence against government overreaching even when the third-party doctrine does not.

but when is warrant needed vs a subpoena

Conclusion

This Article has argued for a new understanding of the third-party doctrine. Critics of the doctrine portray it as a choice between all or nothing, between Fourth Amendment protection or no protection at all.[207] In their view, the third-party doctrine cases "make[] a mockery of the Fourth Amendment,"[208] leaving a constitutional void that is both illogical and inconsistent with a free society.[209] This Article has suggested that this widely held view tells only half the story. The third-party doctrine serves two important roles: blocking substitution effects that upset the technological neutrality of Fourth Amendment law and furthering clarity of Fourth Amendment rules. Further, the effects of the doctrine are much less dire than critics tend to suggest; the doctrine is only one tool among many for addressing abuses of third parties.

In short, both the costs and benefits of the third-party doctrine must account for substitution effects. On the cost side, fears of excessive government power must be offset by the substitution effects of doctrines like entrapment, common law privileges, statutory protections, and the *Massiah* doctrine. On the benefit side, courts should consider how the substitution

---

203. *In re* Grand Jury Subpoena to Amazon.com Dated Aug. 7, 2006, 246 F.R.D. 570, 573 (W.D. Wis. 2007).

204. *See generally* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. Rev. 112 (2007) (exploring the relationship between the First Amendment and criminal procedure).

205. *See, e.g.*, Jason DeParle, *Deal Close on Wiretap Law, a Top Democrat Tells CNN*, N.Y. Times, Mar. 3, 2008, at A13. Of course, by the time this Article is published, this story will be "old news"!

206. *See generally* Orin S. Kerr, Civil Liability and the NSA Call Records Program, http://www.orinkerr.com/2006/05/12/civil-liability-and-the-nsa-call-records-program/ (May 12, 2006, 17:00 EST).

207. *See supra* Section I.B.

208. 1 LaFave, *supra* note 7, § 2.7(b), at 736.

209. *See supra* Section I.B.

effects of third-party services can upset the traditional balance of Fourth Amendment rules. A full appreciation of the role of the third-party doctrine reveals it as much more complicated than critics have claimed. This does not mean that every application of the doctrine is indisputably correct; there is room for disagreement in specific cases, especially given the difficulty of weighing the costs and benefits involved. But when the entire picture is understood, the third-party doctrine has an important place within a proper system of criminal procedure rules.

More broadly, the role of the third-party doctrine reveals an all-too-common blind spot among criminal procedure scholars. Critics have often focused on powers of the government to harass innocent individuals, and have looked for ways that the Constitution can block the harassment.[210] But the Justices of the Supreme Court do not have this luxury. They must create rules that apply for investigations of both the innocent and the guilty in a world in which the government often cannot distinguish the two at the outset. They must look systemically to generate a set of rules that will apply to both.

From this perspective, the Fourth Amendment's warrant requirement is strong medicine—sometimes too strong. True, it deters abuse, but it also stops legitimate good faith investigations. At the preliminary stages of investigations, the police must have tools to gather evidence to determine if probable cause exists; the warrant requirement can then be saved for limiting more invasive practices like searches of homes and packages. While this removes Fourth Amendment scrutiny from a set of third-party practices, it tends to do so when the practices are essentially transactional—a matter of who did what, not what someone was thinking or saying or feeling. Other sources of privacy law can then fill the gap, deterring against abusive practices without imposing the high threshold of the Fourth Amendment's warrant requirement. The result is a system of procedural rules that both protects the innocent and permits investigations and prosecutions of the guilty.

Unfortunately, the Supreme Court has failed miserably at articulating these principles. When faced with the facts of specific cases, the Court has reached results that I think are correct. But by lodging the issue incorrectly in the reasonable expectation of privacy test instead of consent law, the Court has backed itself into a rhetorical corner and left the doctrine largely unexplained. The importance of third-party records in new technologies and the continuing criticisms of the Court's case law suggest that the time has come for courts and commentators alike to develop a more sophisticated understanding of the third-party doctrine. The doctrine should be recast rather than cast aside.

---

210. *See supra* notes 5–11 and accompanying text.

Read 11/3 opt

Kerr Defends the Third-Party Doctrine

by Jim Harper on May 30, 2008 · 2 Comments

Orin Kerr is a law professor at George Washington University and a blogger on the popular Volokh Conspiracy. He is a thoughtful, open-minded legal scholar, but I don't think it's unfair to say that he reliably sides with law enforcement on Fourth Amendment issues.

He recently posted a draft article defending the third-party doctrine, which is an interpretation of the Fourth Amendment holding that a person sharing information with a third party cannot make a Fourth Amendment claim to protection of that information. Use an ISP to transmit your email? No Fourth Amendment protection for its contents. Have a bank account? No Fourth Amendment protection for your banking records. Etc.

He treats as similar two issues that I see as separate: revelations gleaned from informants/agents and from business records. I have always thought of the third-party doctrine as being about business records. My remarks here apply to that area only.

I think the third-party doctrine was never right, and that it grows more wrong with each step forward in modern, connected living. Incredibly deep reservoirs of information are constantly collected by third-party service providers today. Cellular telephone networks pinpoint customers' locations throughout the day through the movement of their phones. Internet service providers maintain copies of huge swaths of the information that crosses their networks, tied to customer identifiers. Search engines maintain logs of searches that can be correlated to specific computers and usually the individuals that use them. Payment systems record each instance of commerce, and the time and place it occurred. The third-party doctrine exempts law enforcement from the Fourth Amendment's reasonableness and warrant requirements when it looks at these records.

It's wonderfully contrarian to run against the grain and defend the third-party doctrine, which has plenty of detractors, but sometimes contrarians can be wrong. I think Professor Kerr is, and here I'll briefly lay out a few of the fundamental differences I have with his paper—all toward the end of perfecting it before it's published in the *Michigan Law Review* next year, of course!

The basic gist of the article is that the third-party doctrine is better than most people think, for two reasons. First, it's technologically neutral. It prevents criminals from making opportunistic use of technology to circumvent the basic balance between security and privacy struck by the Fourth

Amendment. Second, it's easier to administer than alternatives. The arguments against the third-party doctrine are weaker than most people believe, Kerr says. Rather than wedging the third-party doctrine into the "reasonable expectation of privacy" framework arising out of *Katz v. United States*, Kerr argues that the third-party doctrine should be thought of as a form of consent. People sharing information with others are consenting to have it searched.

To make the third-party doctrine more palatable, he argues that substitutes for it help control against abusive practices. These include common law privileges, entrapment law, the *Massiah* doctrine, First Amendment doctrine, statutory privacy protections, and the rights of third parties themselves.

My differences with Kerr are plentiful. Starting at the 30,000 foot level, my sense is that Kerr is treating the Fourth Amendment as a rule about criminal procedure. Oh sure, it's classed that way in the legal academy, it has most of its application in criminal cases, and I first studied Fourth Amendment law in my constitutional criminal procedure class. But add this to the list of things I didn't learn in law school: The touchstone of the Fourth Amendment is the security of the people—all of them—against unreasonable searches and seizures of their persons, houses, papers and effects. "The people" refers to all of us, the law-abiding citizens.

(Kerr's argument that the third-party doctrine is preferable because it's easy to administer holds no weight if the rule derogates from the security of the people, and I'm confident that courts and police departments could manage other rules. That's all I'll have to say on that point so I can focus on Kerr's point about technological neutrality.)

The interplay of the Fourth Amendment and technology is interesting, but I don't think technological neutrality is a terribly relevant or useful metric for Fourth Amendment doctrine. Since the Fourth Amendment was adopted, technology has certainly shifted the scope of human enterprise. I imagine that in the late 1700's most everything of deep import to people's lives—personal and professional—happened in or near the home, so it was natural that the home was a place of high Fourth Amendment protection, and "home" was a useful proxy for "what should be protected."

Since then, technological changes of all kinds have given us the freedom to take our lives outward. We move around much more within our communities and from one to another; we stay in different places and move our residences much more often; we communicate and transact using new technologies; and our things—both tangible and digital—come to rest many more places than they used to.

Focusing on technological neutrality would move our attention off the thing that matters—the security of the people—to whatever privacy people got in the late 1700's from the buildings they constructed around themselves and lived in. Housing was the technology of the time. It was both the locus of activity and the source of security in persons, papers, and effects. (Thanks to the Fourth Amendment, it provided equal security against others as against the government.) It would be odd to let the technology of that time set the standard. Was there something special about the technology of that particular time that affixed the scope of people's rights? Why weren't they set in the era of the caveman? Or . . . 1957?

In 1967, of course, the *Katz* Court recognized that the expanded scope of human action needed coordinate expansion of Fourth Amendment protection, and it said in famous language, "the Fourth Amendment protects people, not places." *Katz* preserved the security of the people as the technology moved their lives from "inside houses" to "on the phone" and elsewhere.

(It's interesting to note how many times Kerr refers to the Fourth Amendment as protecting places: "Fourth Amendment protection for information matches the Fourth Amendment protection for the environment in which it is stored." He could almost be arguing to undo *Katz*.)

The welcome vision displayed in *Katz* counsels that the Fourth Amendment should naturally protect people as they come to use other instrumentalities—automated machinery owned by third parties, in particular—to expand the scope of their lives yet again.

Kerr spends a good deal of time explaining how third parties like phone companies, ISPs, online banks, and such allow people to hide illegal behavior that would otherwise take place in public. But this is true of every technology. Fourth Amendment protection for houses allowed criminals to use houses in concealment of crime rather than planning crime in open fields as they otherwise would have had to do. The thing is, letting the vast majority of honest people be confident in the security of their houses has had more benefits than the costs of letting criminals make use of that protection for crime. This will be true of nearly every technology.

Technological neutrality isn't really relevant. What's relevant is preserving the same security for people and their stuff that they should have in a free society. It's a consistent level of this security that matters—not technological neutrality.

A theme unfortunately *not* running through Kerr's paper is how much it's oriented toward victimless crimes, which require much more surveillance than real crime. At one point, he tellingly refers to crime as "the transaction," not "the theft" or "the murder" or anything like that—"the transaction." He's talking about money laundering, prostitution, gambling, bootlegging, and the like.

Real crimes have complainants who tell the police. There isn't a problem with discovering these crimes or knowing where to start looking for the criminals. The third-party doctrine is intimately bound up with the War on Drugs. Kerr should surface this and grant forthrightly that the third-party doctrine exists for and because of victimless crime laws.

It's a fascinating idea—and weird—that sharing information with a third party is a form of consent to it being searched by the government. This area deserves more thinking, but my initial impression is that the word "consent" loses the moorings that make it meaningful if consent to a search is imputed to any sharing of information.

The consent argument, and much of Kerr's other points are bound up with the "reasonable expectation of privacy" doctrine that evolved from *Katz*. Rather than go through everything now—as I write, it happens to be Friday a little after 5:00 p.m.—I'll just mention that I have an article coming out soon in the *American University Law Review* showing that the "reasonable expectation of privacy" test from Justice Harlan's concurrence is not even supported by the majority's holding in that case.

There is much more to know about privacy. Kerr treats lost privacy and official abuse as essentially the same, though they're quite different. (Two chapters in my book on identification policy discuss the free-standing importance of privacy and anonymity.) So many people have thrown themselves onto the "reasonable expectation of privacy" pyre based on that well-intended but mistaken concurrence. It won't have to happen any more once my article comes out.

I'm going to send Professor Kerr an advance copy. Perhaps the final version of his article will sparkle from the exposure to it!

Commercial Privacy

10/25

Very confusing area

People think important

But no one has a handle on it

King Ballak →

Magician Balam

Looked at Israelites camped down

Why was he converted

Tents askew

So each has privacy

2 traditions,

Brandices' Law review article

Right to be left alone

No roots in fund. legal documents

(2)

From right of freedom of association

State of Alabama vs NAACP

State wanted membership list

So people don't feel chilled

Privacy as common law tort

4 factors

Not used all that much

Questions don't get much help from Torts

Harm must be shown

Must be in $

So courts must be some loss

Present day privacy discussion

1960s - as info systems more + more advanced

Concern about data banks

(3)

How Gov + Commercial orgs might use new found power

So active discussion on what rights should be

↳ Fair Info Pratices

OECD

Info flow + trade

inc info about employees

Biz could exchange info around the world

w/o diff countries

this is still a problem today

- which rules to follow where
- what are your rights in certain place

Us stuck to standard

EU upped rules

(4)

90s → new laws?

No intent → FCC interement authority

Privacy on books + grounds good write up

Adequacy standards of EU

Can't move EU data outside EU unless that country has equiv protections

Does US have adequacy?

Danny: Yes

EU: No

instead US-EU Safe Harbor arrangement

Treaty

Allen: Policy hack/kluge

(5)

Allen FTC's First enforcement action

2 cases Sears + Google

FTC – Ind agency
2 million complaints
internet privacy lastly

What pratices should FTC look at
- unfair + deceptive practices
  Competition

FTC construes narrowly
looks at real harm
not really unfair pratices on Internet
Danny: want Consumers to rely on claims companies make
even by mistake

(6)

- misleading
  - to reasnable Consumer - Ruby standard
  - inc Omission
- reasonable
- material
  - does it actually change consumers' action?
  - will they use to decide to use product

Sears

Offered app

'i spy use

Snooped on browser activity

Paid $10

Nielson boxes

'i For study

Part of community

(7)

Hidden in T&C

Not in reasonable lang

People didn't know what dam loading

Hard to uninstall

Didn't know it was running

Online browsing

1. Complaint
   FTC own brief / allegations
2. Order
   had to distroy all data
   had to display a bunch of info
   phone line to uninstall
   must submit report
   clearly disclose
   box must be unchecked

└ we violated your privacy

(8)

20 years

Negotiated by FTC + Sears

Bad for brand if sued by FTC

If fine → how much does that help consumers?

Fighting in court does happen

↳ talk about in negotiations

how outline of this is shaped

Courts rule on what is unfair

CEO + Boards look at + approve

Anyone can file a complaint

Civil / class action sep

much harder to show harm

(9)

They can continue to offer as long as they fully disclose

Google Buzz

Allen: Can we talk about something else besides my low moments?

Social networking site like Twitter & FB
But automatically enrolled
Most freq contacts public

Orkut: Brazil, Iran, India
Why: First mover + network effects
Losing steam
Named after a developer at Google

How to jump start a social network
We have a social graph

Not clear opt in/opt out

(10)

Not adquate comm to user
Not told made public
Or buried/not clear
Hav create lists of followers/who could see
Default public → had to change
hard to find

Lots of precheded box
There were users who really liked it
Automatic connection w/ Picassa + Google Reader

Whole set of changes Google makes
2 waves of changes in first few days

- Defn of what clearly means
- Audits/Assessments
- No misrepresentation
- Privacy by design ← novel
  - Hire people responsible for

(11)

Big deal → any time disclose info for diff reason then before

? that was. huge change

FB can do

But Google can't

Since sep/express permission

20 years!

Allen: difficult to tie down

What becomes natural in 20 years

All Google wide!

See how these things evolve

No one admits to rule breaking

But good facts

FTC has roots in Trust busting The Jungle era

Was not controversial at the time

(12)

More rules than caveat emptor contract law
Consumer Protection Agency provides more protection

How does something like this happen?
How did they screw up?

Google judges APM on launch + get users
- early + often
- fear ~~of~~ of competive

Allen: Huge wake up call
Helpful

Disaster
Huge amt of work to fix
Many other things going on
China thing
Policy + legal team on that
Launched w/o vetting

(13)

Is disclosure enough?

Commission Staff tries to follow trend

Will do pre-briefs

Get pre signal
launch

EU too

Q: Can you renegotiate

Eric Schmidt asked too

FB, Twitter has one too

They don't know market 5 years from now

Ironclad

Odds pretty low

Pretty much industry standards

(14)

Allen: Good medicine for Google
as long as everyone else must do
FTC also
Danny: Competition
So staff still gets preview

Info confidential
but staff leaks, leaves
But relationships matter

Product Liability have really changed practices
Class action

Easier to show damages
All of these are ~~dont~~ Services → not prod liability
Must be higher legal standard

Will we ever address license is not a product
Standards are very different

(15)

FTC moved into critical position
Not under FCC

Danny's Work in Gov

↳ Decision to look at privacy
Becoming more important

Strenghts

All in Blueprint paper
Green paper = draft

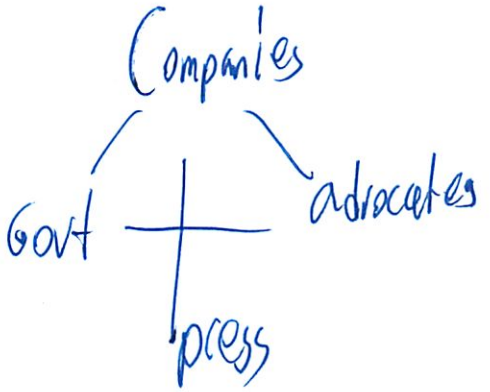
a) sector-specific
too many privacy laws?
Internet was at start unregulated

b) flexible
Google could not have done Gmail

Do we have right protections?
Do we allow econ to grow

(16)

Privacy on grand diff than law describes



? European commissioner envious about press doing investigations - like at WSJ

Stories that have led to investigations

But out of messy process emerges rules

Weaknesses

a) mixed incentive to participate
if no brand diff
no one heard of your Co
just meet the promises you made

(17)

b) lack of clarity of FTC authority

c) lack of global standard

EU mostly regulate US companies

Since US Cos dominate

better treatment if more integrated in European market

So to fix.

1. Legislation what FTC can/can't do

Consumer Privacy Bill of Rights

2. Flexibly implement (missed)

3. Global interoperability EU unlikely to change their view

Europe's law has viral effect

Need a privacy law like ours

(18)

So many countries do EU laws
ie Copied types
So not deliberate legislative process
European framework just applied

EU not as much as biz stake

FTC doing majority of privacy for the world
w/ all the consent decrees
doing privacy for world

Europe raised standards

CNIL - reaction to new Google Privacy Policy

Dunny i light handed
Other stuff issues orders

Break

(19)

Groups

1 Google as a Co
2. Internet / Ad industry
3. FB/Twitter / Apple
4. Progressive privacy adv
5. Libertarian/Conservative
6. US Congress
7. White House

Was a libertarian article

↑ Protection against gov privacy intrusion

And make no rules against busines

State of limitation against gov

(20)

traditional libertarian vs civil libertarianism

↓ economic
no gov intervention in marketing

↓ more about privacy
inc from big co

like mandatory age verification
User self empowerment

ACLU
Eff
Valve choice

---

informed consent required
inc exchanges
consumer protection laws ← very against them
but do like trust
so mixed on informed consent

(4)

Prob mixed bc

↳ if anything → informed choice

empower consumers the most

Given the choice

↳ allow you to protect yourself

Don't like abortion informed consent

: Like cigarette ads

(forgot one)

Groups

1. Google

most import FAQ

(basically screen ya)

2. Ad

Certifies w/ use data

(27)

(we didn't tie back to cihl)

3. Other Interest Cos
   (lwity
   (BS)
   Allen i will ya be next?
   (Throwing them under the bus)
   ?Ben's excuse for target

4. disclosure + consent
   Stronger enforcement
   more rules

5. Us
   (no comments)

(23)

6. Congress

Privacy

but not detrimental to privacy

7. White House

Easy to access + easy to read

But should have flexibility

Europe should not be seen as one

~~II~~

France was chosen to represent privacy

Italy very strict on law

Germany → then Google might withdraw out of Europe

France wrapped this up in a week

more mild

Germany still negotiating over wifi

EU

Rest of EU likes how France is approaching problem
Germany unhappy — wanted to negotiate

EU trying to standardize
so easier for European countries

Allen: Googles' new policy was
lets be very open
But ran into EU problem

But I left Google before this

Next week Moot Court
like Congressional hearing
Grand 3rd party Bar doctine
facts posted tmw
get feel of justice + flow of arguments

25

Be clear about legal rules + facts of case that apply

Clarence Thomas must task be a qu

IRAC:

Intro
Rule
Analysis
Conclusion

for brief/mems

Sometimes legal opinion

Brief: Make argument