Read WSJ index

GUIDELINES FOR ACCESS, RETENTION, USE, AND DISSEMINATION BY THE NATIONAL COUNTERTERRORISM CENTER AND OTHER AGENCIES OF INFORMATION IN DATASETS CONTAINING NON-TERRORISM INFORMATION

I. Background

A. Pursuant to section 119(d) of the National Security Act of 1947, as amended, the National Counterterrorism Center (NCTC) shall "serve as the primary organization in the United States Government for analyzing and integrating all intelligence possessed or acquired by the United States Government pertaining to terrorism and counterterrorism, excepting intelligence pertaining exclusively to domestic terrorists and domestic counterterrorism." NCTC shall also "serve as the central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support"; ensure that agencies "have access to and receive all-source intelligence support needed to execute their counterterrorism plans or perform independent, alternative analysis"; and "ensure that such agencies have access to and receive intelligence needed to accomplish their assigned activities." Furthermore, any agency "authorized to conduct counterterrorism activities may request information" from NCTC "to assist it in its responsibilities." *Id.* § 119(e)(2). Finally, the Director of National Intelligence (DNI) also has significant responsibilities for information sharing. He has "principal authority to ensure maximum availability of and access to intelligence information" within the Intelligence Community (IC). *Id.* § 102A(g)(1). When he establishes standards for facilitating access to and dissemination of information and intelligence, the DNI should give "the highest priority to detecting, preventing, preempting and disrupting terrorist threats and activities." Executive Order 12333 § 1.3(b)(6)(A).

B. NCTC's analytic and integration efforts concerning terrorism and counterterrorism, as well as its role as the central and shared knowledge bank for known and suspected terrorists, at times require it to access and review datasets that are identified as including non-terrorism information in order to identify and obtain "terrorism information," as defined in section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, as amended.[1] "Non-

[1] "The term 'terrorism information'—
(A) means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to—
(i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;
(ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;
(iii) communications of or by such groups or individuals; or
(iv) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and
(B) includes weapons of mass destruction information." 6 U.S.C. § 485(a)(5).

terrorism information" for purposes of these Guidelines includes information pertaining exclusively to domestic terrorism, as well as information maintained by other executive departments and agencies that has not been identified as "terrorism information" as defined by IRTPA. Included within those datasets identified as including non-terrorism information may be information concerning "United States persons," as defined in Executive Order 12333 of December 4, 1981, as amended. The President authorized the sharing of terrorism information in Executive Order 13388 of October 25, 2005, and required that agencies place the "highest priority" on the "interchange of terrorism information" in order to "strengthen the effective conduct of United States counterterrorism activities and protect the territory, people, and interests of the United States of America." That order further requires that the "head of each agency that possesses or acquires terrorism information . . . shall promptly give access to the terrorism information to the head of each other agency that has counterterrorism functions, and provide the terrorism information to each such agency," consistent with law and statutory responsibilities. In the National Security Act of 1947, as amended, Congress recognized that NCTC must have access to a broader range of information than it has primary authority to analyze and integrate if it is to achieve its missions. The Act thus provides that NCTC "may, consistent with applicable law, the direction of the President, and the guidelines referred to in section 102A(b), receive intelligence pertaining exclusively to domestic counterterrorism from any Federal, State, or local government or other source necessary to fulfill its responsibilities and retain and disseminate such intelligence." National Security Act of 1947, as amended, § 119(e). Further, the Act envisions that NCTC, as part of the Office of the Director of National Intelligence (ODNI), *id.* § 119(a), would have the broadest possible access to national intelligence relevant to terrorism and counterterrorism. Section 102A(b) of the National Security Act of 1947, as amended, provides that "[u]nless otherwise directed by the President, the Director of National Intelligence shall have access to all national intelligence and intelligence related to the national security which is collected by any federal department, agency, or other entity, except as otherwise provided by law or, as appropriate, under guidelines agreed upon by the Attorney General and the Director of National Intelligence."

C. These Guidelines are established between the Attorney General and the Director of National Intelligence pursuant to section 102A(b) of the National Security Act of 1947, as amended, to govern the access, retention, use, and dissemination by NCTC of terrorism information that is contained within datasets maintained within other executive departments or agencies that are identified as including non-terrorism information. These Guidelines do not supersede the arrangements in place under the Memorandum of Agreement for the Interagency Threat Assessment and Coordination Group (ITACG). *See* Homeland Security Act of 2002, as amended, section 210D, and the September 27, 2007 Memorandum of Agreement on the Establishment and Operation of the Interagency Threat Assessment and Coordination Group (hereinafter the "ITACG MOA"). The procedures for the ITACG MOA will be implemented consistent with these Guidelines. These Guidelines also constitute procedures pursuant to section 2.3 of Executive Order 12333 for NCTC's access to and acquisition of data concerning United States persons within the datasets explicitly covered by these Guidelines, and the retention and dissemination of such information from these datasets. The Attorney General-approved procedures pursuant to section 2.3 generally governing NCTC's and ODNI's access and acquisition activities (reference (o), below) are hereby superseded insofar as they apply to

NCTC's retention, use, and dissemination of data and datasets governed by these Guidelines. NCTC's retention, use, and dissemination of information contained in the datasets governed by these Guidelines and all other NCTC activities remain subject to all other applicable laws and regulations. The terms and conditions of each specific information access or acquisition (hereinafter "Terms and Conditions") from another department or agency (hereinafter a "data provider") shall be developed in accordance with the provisions in section III.B.2 below, and shall be consistent with the Information Sharing Environment (ISE) guidelines issued pursuant to section 1016 of the IRTPA, to include the guidelines to protect privacy and civil liberties in the development and use of the information sharing environment.

II. References

a) National Security Act of 1947, as amended
b) Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, as amended
c) Homeland Security Act of 2002, as amended
d) Federal Agency Data Mining Reporting Act of 2007 (42 U.S.C. § 2000ee-3)
e) 18 U.S.C. § 2332b(f) (Acts of terrorism transcending national boundaries—investigative authority)
f) Executive Order 12333 of December 4, 1981, as amended, "United States Intelligence Activities"
g) Executive Order 13388 of October 25, 2005, "Further Strengthening the Sharing of Terrorism Information to Protect Americans"
h) Intelligence Community Directive (ICD) 501 of January 21, 2009, "Discovery and Dissemination or Retrieval of Information within the Intelligence Community"
i) ICD 503 of September 15, 2008, "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation"
j) Director of Central Intelligence Directive (DCID) 6/3 of June 5, 1999, "Protecting Sensitive Compartmented Information within Information Systems," appendix E (or successor ICD and Policies)
k) DCID 6/6 of July 11, 2001, "Security Controls on the Dissemination of Intelligence Information," (or successor ICD and Policies)
l) December 4, 2006 Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment
m) March 4, 2003 Memorandum of Understanding Between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing
n) September 27, 2007 Memorandum of Agreement on the Establishment and Operation of the Interagency Threat Assessment and Coordination Group
o) The Attorney General-approved procedures promulgated through Central Intelligence Agency Headquarters Regulation 7-1 of December 23, 1987, "Law and Policy Governing the Conduct of Intelligence Activities," as adopted by ODNI/NCTC, including any successor procedures (hereinafter "NCTC's EO 12333, § 2.3 Procedures")
p) National Counterterrorism Center Information Sharing Policy of February 27, 2006, "Rules of the Road" (NCTC Policy Document 11.2) (or successor Policy)

q) National Counterterrorism Center Role-Based Access Policy of July 13, 2009 (NCTC Policy Document 11.7) (or successor Policy)
r) ODNI Instruction 80.05, Implementation of Privacy Guidelines for Sharing Protected Information, September 2, 2009 (hereinafter "ODNI ISE Privacy Instruction")
s) ODNI Instruction 80.02, Managing Breaches of Personally Identifiable Information, February 20, 2008.

III. Guidelines

A. Authority for and Scope of NCTC Data Access and Acquisitions

1. *Purpose and Authority.* NCTC's access to, and acquisition, retention, use, and dissemination of, information covered by these Guidelines will be for authorized NCTC purposes. Pursuant to Executive Order 13388 and consistent with the National Security Act of 1947, as amended, and the March 4, 2003 Memorandum of Understanding between the Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing, NCTC shall be afforded prompt access to all federal information and datasets that may constitute or contain terrorism information. NCTC may access or acquire datasets that may constitute or contain terrorism information, including those identified as containing non-terrorism information, such as information pertaining exclusively to domestic terrorism and other information maintained by executive departments and agencies that has not been identified as terrorism information, in order to acquire, retain, and disseminate terrorism information pursuant to NCTC's statutory authorities consistent with these Guidelines.

2. *United States Person Information.* These Guidelines permit NCTC to access and acquire United States person information for the purpose of determining whether the information is reasonably believed to constitute terrorism information and thus may be permanently retained,[2] used, and disseminated. Any United States person information acquired must be reviewed for such purpose in accordance with the procedures below. Information is "reasonably believed to constitute terrorism information" if, based on the knowledge and experience of counterterrorism analysts as well as the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the information is terrorism information.

3. *Erroneously Provided Information and Errors in Information.* Any United States person information that has been erroneously provided to NCTC will not be retained, used, or disseminated by NCTC. Such information will be promptly removed from NCTC's systems, unless such removal is otherwise prohibited by applicable law or court order or by regulation or policy approved by the Attorney General. Information in NCTC systems found to contain errors will be promptly corrected to ensure information integrity and accuracy, and the data provider shall be notified of the error when feasible.

[2] For purposes of these Guidelines, "permanently retained" does not mean that the information is retained indefinitely, but rather that it is retained in accordance with NCTC's records retention policies.

4. *Applicable Laws and Policies.*

a) NCTC will access, acquire, retain, use, and disseminate information, including United States person information, (i) pursuant to the relevant standards of Executive Order 12333, as amended; (ii) as consistent with the National Security Act of 1947, as amended; and (iii) as authorized by law or regulations, including applicable privacy laws. These Guidelines do not apply to information the retention, use, and dissemination of which is governed by court order or court-approved procedures.

b) NCTC shall not access, acquire, retain, use, or disseminate United States person information solely for the purpose of monitoring activities protected by the First Amendment or monitoring the lawful exercise of other rights secured by the Constitution or other laws of the United States. NCTC users of acquired information will be subject at all times to NCTC's Role-Based Access and Information Sharing Policies, to applicable ODNI Instructions, and to additional audit and oversight authorities and requirements, as applicable. In implementing these Guidelines, NCTC shall consult with the ODNI General Counsel and the ODNI Civil Liberties Protection Officer, as appropriate.

5. *Responsibility for Compliance.* The Director of NCTC, in consultation with the ODNI Office of General Counsel, shall be the responsible official for ensuring that NCTC complies with these Guidelines. The ODNI Civil Liberties Protection Officer shall oversee compliance with these Guidelines and compliance with other applicable laws, regulations, guidelines, and instructions as they relate to civil liberties and privacy.

B. General Procedures for NCTC Data Access and Acquisitions

1. *Identification of Datasets.* NCTC will coordinate with the data provider to identify datasets that are reasonably believed to contain terrorism information, including those identified as containing non-terrorism information.

2. *Establishing Terms and Conditions for Information Access.*

a) For access to or acquisition of specific datasets, the DNI, or the DNI's designee, shall collaborate with the data provider to identify any legal constraints, operational considerations, privacy or civil rights or civil liberties concerns and protections, or other issues, and to develop appropriate Terms and Conditions that will govern NCTC's access to or acquisition of datasets under these Guidelines. If either party believes that the Terms and Conditions do not adequately address the matters identified during that collaboration, that party may raise those concerns in accordance with the procedures in section III.B.2(d), below. These Guidelines do not alter any other obligations of a data provider to provide information to the DNI or NCTC. All Terms and Conditions shall incorporate these Attorney General-approved Guidelines, and shall ensure that information is transmitted, stored, retained, accessed, used, and disseminated in a manner that (i) protects privacy and civil liberties and information integrity and security, and (ii) is in accordance with applicable laws, regulations, guidelines and instructions (including the ODNI ISE Privacy Instruction). NCTC and the data provider will establish procedures to ensure the

data provider notifies NCTC of any information the data provider believes, or subsequently determines to be, materially inaccurate or unreliable. NCTC will ensure mechanisms are in place at NCTC to correct or document the inaccuracy or unreliability of such information, and supplement incomplete information to the extent additional information becomes available. NCTC will work with the data provider to ensure that data acquired by NCTC under these Guidelines is updated and verified throughout its retention and use by NCTC, in accordance with the data quality, data notice, redress, and other applicable provisions of the ODNI ISE Privacy Instruction.

b) NCTC shall consult with the data provider to identify and put in place additional measures as necessary to honor obligations under applicable international agreements governing the information.

c) Any safeguards, procedures, or oversight mechanisms that go beyond those specified in these Guidelines shall be documented in the Terms and Conditions, and may include protections for sensitive sources and methods, pending investigations, law enforcement equities, foreign government interests, privacy and civil liberties, and similar considerations that apply to the use of the information. Any additional protective measures – such as the degree of advance coordination, if any, for dissemination of information obtained from a data provider – shall also be specified in the Terms and Conditions.

d) If the head of the department or agency providing the information or the DNI objects to providing data to NCTC, objects to the "track" under which NCTC intends to acquire the data, or objects to the Terms and Conditions developed after consultation (*e.g.*, he or she believes that the Terms and Conditions do not adequately ensure that information is transmitted, stored, retained, accessed, used, and disseminated in a manner that protects privacy and civil liberties and information integrity and security; do not adequately addresses operational equities; unnecessarily restrict sharing and use of the information; or are not in accordance with applicable laws, international agreements, and regulations), the head of the department or agency or the DNI may raise any concerns, in writing, with the other party. The head of the department or agency and the DNI shall attempt to resolve any such concern. Failing resolution, either party may refer a dispute concerning constitutional or other legal matters to the Attorney General and may seek the resolution of any other disputes through the National Security Council process. In connection with such disputes, the Attorney General or National Security Council may seek the advice of the Privacy and Civil Liberties Oversight Board.

3. *Training.* NCTC shall ensure that all NCTC employees, NCTC contractors, and detailees and assignees to NCTC from other agencies (hereinafter "NCTC personnel") provided access to datasets under these Guidelines receive training in the use of each dataset to which they will have access to ensure that these personnel use the datasets only for authorized NCTC purposes and understand the baseline and enhanced safeguards, dissemination restrictions, and other privacy and civil liberties protections they must apply to each such dataset. These personnel will also receive ongoing training to ensure understanding of these Guidelines and civil liberties and privacy expectations and requirements involved in the access to and use of datasets governed by

these Guidelines. The training required by this paragraph shall be in person whenever practicable and refreshed at least annually.

4. *Authorized Uses of Information.* Subject to any additional protections, requirements, or provisions in applicable Terms and Conditions, terrorism information, including terrorism information concerning United States persons, properly acquired and retained by NCTC may be used for all authorized NCTC purposes. These include, but are not limited to: analysis and integration purposes, inclusion in finished analytic products and pieces, enhancement of records contained within the Terrorist Identities Datamart Environment (TIDE), operational support, strategic operational planning, and appropriate dissemination to Intelligence Community elements, as well as federal and other counterterrorism partners. Specific provisions on use and dissemination are set forth in sections III.C and IV below, and any additional protections or provisions shall be specified in the Terms and Conditions.

5. *Information Access Requests.* For information acquired pursuant to the tracks outlined in section III.C below, it shall be the responsibility of the data provider to make determinations regarding the Freedom of Information Act and first-party access under the Privacy Act, and discovery or other requests for such information in any legal proceeding, unless a different arrangement is agreed upon between NCTC and the data provider and specified in the Terms and Conditions or is required by law. Information derived from an operational file exempted from search and review, publication, and disclosure under 5 U.S.C. § 552 in accordance with law shall remain under the control of the data provider and be handled as coordinated in advance with the data provider and specified in the Terms and Conditions for that information.

C. Specific Procedures for NCTC Data Access and Acquisitions

General. NCTC may acquire information contained within datasets governed by these Guidelines in one or more of the three ways outlined below. NCTC, in coordination with the data providers, will determine which information acquisition track, or tracks, provides the most effective means of ensuring NCTC access to terrorism information contained in the relevant datasets, consistent with the protection of privacy and civil liberties of United States persons, and any applicable legal requirements affecting provision of the specific data.

1. Track 1 Information Acquisition: Account-Based Access

a) *Type of Access.* NCTC personnel may be provided account-based access to the datasets of data providers that contain or may contain terrorism information (hereinafter "Track 1" access).

b) *Standard.* NCTC will access information in such datasets identified as containing non-terrorism information only to determine if the dataset contains terrorism information. NCTC may acquire, retain, use, and disseminate terrorism information for all authorized NCTC purposes, as described in these Guidelines. If the information acquired by NCTC is subsequently determined not to constitute terrorism information, NCTC will promptly purge any information the retention, use, or dissemination of which is not authorized by sections IV and V below.

c) *Terrorism Datapoints.* Consistent with section 119 of the National Security Act of 1947, as amended, and section 1016(a)(5) of the IRTPA, as amended, the initial query term for NCTC Track 1 access shall be a known or suspected terrorist identifier or other piece of terrorism information (hereinafter "terrorism datapoints"). In order to follow up on positive query results, subsequent terrorism datapoints may be used to explore a known or suspected terrorist's network of contacts and support. NCTC's activities in Track 1 shall be designed to identify information that is reasonably believed to constitute terrorism information. NCTC is not otherwise permitted under these Guidelines to query, use, or exploit such datasets. For example, analysts may not browse through records in the dataset that do not match a query with terrorism datapoints, or conduct pattern-based queries or analyses without terrorism datapoints.

d) *Protection of Sources and Methods.* NCTC shall work with the data provider to ensure that terrorism datapoints and matching records from the dataset are provided, received, stored, and used in a secure manner that appropriately protects intelligence sources and methods and related sensitivities, consistent with the requirements of Appendix E of DCID 6/3 and ICD 503, or successor ICD.

2. Track 2 Information Acquisition: Search and Retention

a) *Type of Access.* NCTC may provide the owner of a dataset that contains or that may contain terrorism information with query terms – either singly or in batches – consisting of terrorism datapoints so that a search of the dataset may be run (hereinafter "Track 2" access).

b) *Standard.* Information from the dataset that is responsive to queries using NCTC-provided terrorism datapoints will be given by the data provider to NCTC. NCTC may acquire, retain, use, and disseminate information acquired under Track 2 for all authorized NCTC purposes, as described in these Guidelines. NCTC's activities in Track 2 shall be designed solely to identify information that is reasonably believed to be terrorism information. If the information given by a data provider to NCTC does not constitute terrorism information, NCTC will promptly purge any information whose retention, use, or dissemination is not authorized by sections IV and V below.

c) *Protection of Sources and Methods.* NCTC shall work with the data provider to ensure that terrorism datapoints and responsive records from the dataset are provided, received, stored, and used in a secure manner that appropriately protects intelligence sources and methods and related sensitivities, consistent with the requirements of DCID 6/3 and ICD 503, or successor ICD.

3. Track 3 Information Acquisition: NCTC Dataset Acquisition

a) *Type of Access.* NCTC may acquire and replicate portions or the entirety of a dataset when necessary to identify the information that constitutes terrorism information within the dataset (hereinafter "Track 3" access).

b) *Standard and Process.* Replication of data is appropriate when the Director of NCTC, or a designee who serves as Principal Deputy Director or as a Deputy Director (hereinafter "Designee"), determines in writing, after coordination with the data provider, that a dataset is

likely to contain significant terrorism information and that NCTC's authorized purposes cannot effectively be served through Tracks 1 or 2. When making a determination, the Director or Designee also shall consider whether NCTC's authorized purposes can effectively be served by the replication of a portion of a dataset. Datasets received in accordance with Track 3 may not be accessed or used by NCTC prior to replication, except as directly necessary to make the determination above or to accomplish such replication, subject to procedures agreed upon with the data provider. Measures will be put in place to ensure that the dataset is received and stored in a manner to prevent unauthorized access and use prior to the completion of replication.

c) *Identification of United States Person Information and Temporary Retention Period.* For all datasets received pursuant to Track 3, NCTC will use reasonable measures to identify and mark or tag United States person information contained within those datasets. Any United States person information acquired pursuant to Track 3 may be retained and continually assessed for a period of up to five years by NCTC to determine whether the United States person information is reasonably believed to constitute terrorism information (hereinafter "temporary retention period"). The Terms and Conditions shall establish the temporary retention period for continual assessment of such information. The temporary retention period specified in the Terms and Conditions may be up to five years unless a shorter period is required by law, including any statute, executive order, or regulation. In no event may NCTC retain the information for longer than is permitted by law. The temporary retention period shall commence when the data is made generally available for access and use following both the determination period discussed in section III.C.3(b) immediately above, and any necessary testing and formatting. United States person information that is reasonably believed to constitute terrorism information may be permanently retained and used for all authorized NCTC purposes, as described in these Guidelines.

d) *Baseline Safeguards, Procedures, and Oversight Mechanisms.* During the temporary retention period, the following baseline safeguards, procedures, and oversight mechanisms shall apply to all datasets acquired pursuant to Track 3 that have been determined to contain United States person information:

(1) These datasets will be maintained in a secure, restricted-access repository.

(2) Access to these datasets will be limited to those NCTC personnel who are acting under, and agree to abide by, NCTC's information sharing and use rules, including these Guidelines; who have the requisite security clearance and a need-to-know in the course of their official duties; and who have received the training required by section III.B.3.

(3) Access to these datasets will be monitored, recorded, and audited. This includes tracking of logons and logoffs, file and object manipulation and changes, and queries executed, in accordance with audit and monitoring standards applicable to the Intelligence Community. Audit records will be protected against unauthorized access, modifications, and deletion, and will be retained for a sufficient period to enable verification of compliance with rules applicable to the data for which audit records apply.

(4) NCTC's queries or other activities to assess information contained in datasets acquired pursuant to Track 3 shall be designed solely to identify information that is reasonably believed to constitute terrorism information. NCTC shall query the data in a way designed to minimize the review of information concerning United States persons that does not constitute terrorism information. To identify information reasonably believed to constitute terrorism information contained in Track 3 data, NCTC may conduct (i) queries that do not consist of, or do not consist exclusively of, terrorism data points, and (ii) pattern-based queries and analyses. To the extent that these activities constitute "data mining" as that term is defined in the Federal Agency Data Mining Reporting Act of 2007, the DNI shall report these activities as required by that Act.

(5) NCTC will conduct compliance reviews as described below in section VI.

e) *Enhanced Safeguards, Procedures, and Oversight Mechanisms.* In addition to the requirements of paragraph (d), at the time when NCTC acquires a new dataset or a new portion of a dataset, the Director of NCTC or Designee shall determine, in writing, whether enhanced safeguards, procedures, and oversight mechanisms are needed. In making such a determination, the Director of NCTC or Designee shall (i) consult with the ODNI General Counsel and the ODNI Civil Liberties Protection Officer, and (ii) consider the sensitivity of the data; the purpose for which the data was originally collected by the data provider; the types of queries to be conducted; the means by which the information was acquired; any request or recommendation from the data provider for enhanced safeguards, procedures, or oversight mechanisms; the terms of any applicable international agreement regarding the data; the potential harm or embarrassment to a United States person that could result from improper use or disclosure of the information; practical and technical issues associated with implementing any enhanced safeguards, procedures, or oversight mechanisms; and all other relevant considerations. If the Director of NCTC or Designee determines that enhanced safeguards, procedures, and oversight mechanisms are appropriate, the determination shall include a description of the specific enhanced safeguards, procedures, or oversight mechanisms that will govern the continued retention and assessment of the dataset. These enhanced safeguards, procedures, or oversight mechanisms may include the following:

(1) Additional procedures for review, approval, and/or auditing of any access or searches;

(2) Additional procedures to restrict searches, access, or dissemination, such as procedures limiting the number of personnel with access or authority to search, establishing a requirement for higher-level authorization or review before or after access or search, or requiring a legal review before or after United States person identities are unmasked or disseminated;

(3) Additional use of privacy enhancing technologies or techniques, such as techniques that allow United States person information or other sensitive information to be "discovered" without providing the content of the information, until the appropriate standard is met;

(4) Additional access controls, including data segregation, attribute-based access, or other physical or logical access controls;

(5) Additional, particularized training requirements for NCTC personnel given access or authority to search the dataset; and

(6) More frequent or thorough reviews of retention policies and practices to address the privacy and civil liberties concerns raised by continued retention of the dataset.

Any enhanced safeguards, procedures, and oversight mechanisms must be included in the Terms and Conditions, or specified in writing and appended to the Terms and Conditions, and shall be kept on file as required by NCTC's record retention schedule.

f) *Removal of Information.* NCTC shall remove from NCTC's systems all identified information concerning United States persons that NCTC does not reasonably believe constitutes terrorism information within five years from the date the data is generally available for assessment by NCTC (or within the time period identified in the Terms and Conditions if the Terms and Conditions specify a shorter temporary retention period), unless such removal is otherwise prohibited by applicable law or court order or by regulation or policy approved by the Attorney General, or unless the information is retained for administrative purposes as authorized in section V below.

g) *Protection of Sources and Methods.* NCTC shall work with the data provider to ensure that information for dataset replications is provided, received, stored, and used in a secure manner that appropriately protects intelligence sources and methods and related sensitivities, consistent with the requirements of DCID 6/3 and ICD 503, or successor ICD.

IV. Dissemination

A. General Dissemination Requirements

1. *Definition.* For purposes of these Guidelines, dissemination means transmitting, communicating, sharing, passing, or providing access to information outside NCTC by any means, to include oral, electronic, or physical means.

2. *Terms and Conditions and Privacy Act.* All disseminations under these Guidelines must be: (i) compatible with any applicable Terms and Conditions or, if not compatible, the data provider must have otherwise consented to the dissemination; and (ii) permissible under the Privacy Act, 5 U.S.C. § 552a, if applicable.

3. *Dissemination to State, Local, or Tribal Authorities or Private-Sector Entities.* These Guidelines are not intended to alter or otherwise impact pre-existing information sharing relationships by federal agencies with state, local, or tribal authorities or private-sector entities, whether such relationships arise by law, Presidential Directive, MOU, or other formal agreement (including, but not limited to, those listed in section II above). To the extent that these

Guidelines allow for dissemination to state, local, tribal, or private sector entities, such dissemination will continue to be made, consistent with section 119(f)(1)(E) of the National Security Act (50 U.S.C. § 404o(f)(1)(E)), in support of the Department of Justice (including the FBI) or the Department of Homeland Security responsibilities to disseminate terrorism information to these entities, and conducted under agreements with those Departments.

B. Dissemination of United States Person Information Acquired Under Tracks 1, 2, or 3

NCTC may disseminate United States person information properly acquired under Tracks 1, 2, or 3 if the General Dissemination Requirements are met, and if:

(1) *Dissemination of Terrorism Information.* The United States person information reasonably appears to constitute terrorism information, or reasonably appears to be necessary to understand or assess terrorism information, and NCTC is disseminating the information to a federal, state, local, tribal, or foreign or international entity, or to any other appropriate entity that is reasonably believed to have a need to receive such information for the performance of a lawful function;

(2) *Dissemination for Limited Purposes.* The United States person information is disseminated to other elements of the Intelligence Community or to a federal, state, local, tribal, or foreign or international entity, or to any other appropriate entity, for the limited purpose of assisting NCTC in determining whether the United States person information constitutes terrorism information. Any such recipients may only use the information for this limited purpose, and may not use the information for any other purpose or disseminate the information further without the prior approval of NCTC. Recipients of information under this paragraph must promptly provide the requested assistance to NCTC and promptly thereafter return the information to NCTC or destroy it unless NCTC authorizes continued retention after the specific information is determined by NCTC to meet the dissemination criteria in section IV.C.1 of these Guidelines. Recipients of information under this paragraph may not retain the information for purposes of continual assessment of whether it constitutes terrorism information unless such retention would be permitted by the dissemination criteria in section IV.C.1. Any access to or dissemination under this paragraph of any bulk dataset or significant portion of a dataset believed to contain United States person information must be: (i) approved by the Director of NCTC; and (ii) expressly allowed by the Terms and Conditions or otherwise expressly approved by the data provider. In addition, the recipient of any bulk dataset or significant portion of a dataset under this provision must agree in writing that it: (i) will not disseminate the information further without prior approval by NCTC; (ii) will use the data solely for the limited purpose specified in this provision; (iii) will promptly return the data to NCTC or destroy it after providing the required assistance to NCTC, unless NCTC authorizes continued retention of specific information after it is determined by NCTC to meet the dissemination criteria in section IV.C.1 of these Guidelines; (iv) will comply with any safeguards and procedures deemed appropriate by the ODNI General Counsel and ODNI Civil Liberties Protection Officer; and (v) will

report to NCTC any significant data breach or failure to comply with the terms of its agreement. In deciding whether to approve dissemination under this paragraph of any bulk dataset or significant portion of a dataset, the Director of NCTC shall consider whether the limited purpose of this paragraph can be satisfied by allowing access to the data while it remains under NCTC's control and whether the recipient of the data has the capabilities necessary to comply with the requirements specified above;

(3) *Dissemination Based on Consent.* The United States person whom the information concerns consents to the dissemination; or

(4) *Dissemination of Publicly Available Information.* The United States person information is publicly available.

C. Dissemination of United States Person Information Acquired Under Track 3

1. *Standard (Non-bulk) Dissemination of Specific Information Acquired Under Track 3.* In addition to the provisions above for dissemination under all three tracks, NCTC may disseminate specific United States person information acquired under Track 3 that has been handled and subsequently identified in accordance with applicable Track 3 safeguards and procedures,[3] if the General Dissemination Requirements are met, and if the United States person information:

a) Reasonably appears to be foreign intelligence or counterintelligence, or information concerning foreign aspects of international narcotics activities, or reasonably appears to be necessary to understand or assess foreign intelligence, counterintelligence, or foreign aspects of international narcotics activities, and NCTC is disseminating the information to another federal, state, local, tribal, or foreign or international entity that is reasonably believed to have a need to receive such information for the performance of a lawful function, provided they agree to such further restrictions on dissemination as may be necessary;

b) Reasonably appears to be evidence of a crime, and NCTC is disseminating the information to another federal, state, local, tribal, or foreign agency that is reasonably believed to have jurisdiction or responsibility for the investigation or prosecution to which the information relates and a need to receive such information for the performance of a lawful governmental function;

c) Is disseminated to a Congressional Committee to perform its lawful oversight functions, after approval by the ODNI Office of General Counsel;

d) Is disseminated to a federal, state, local, tribal, or foreign or international entity, or to an individual or entity not part of a government, and is reasonably believed to be necessary to: (i) protect the safety or security of persons, property, or organizations; or

[3] This paragraph does not authorize NCTC to search for the additional categories of information, but rather allows NCTC to disseminate specific United States person information discovered while performing counterterrorism analysis and searches in accordance with these Guidelines and the applicable Terms and Conditions.

(ii) protect against or prevent a crime or a threat to the national security, provided they agree to such further restrictions on dissemination as may be necessary;

e) Is disseminated to another federal, state, local, tribal, or foreign or international entity for the purpose of determining the suitability or credibility of persons who are reasonably believed to be potential sources or contacts, provided they agree to such further restrictions on dissemination as may be necessary;

f) Is disseminated to another federal, state, local, tribal, or foreign or international entity for the purpose of protecting foreign intelligence or counterintelligence sources and methods from unauthorized disclosure;

g) Is disseminated to other recipients, if the subject of the information provides prior consent in writing;

h) Is otherwise required to be disseminated by statutes; treaties; executive orders; Presidential directives; National Security Council directives; Homeland Security Council directives; or Attorney General-approved policies, memoranda of understanding, or agreements; or

i) Is disseminated to appropriate elements of the Intelligence Community for the purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it.

The identity of a United States person may be disseminated outside the Intelligence Community only if it is necessary or if it is reasonably believed that it may become necessary to understand and assess such information.

2. *Bulk Dissemination of Information Acquired Under Track 3 to IC Elements.* If the General Dissemination Requirements in section IV.A above are met, NCTC also may disseminate United States person information acquired under Track 3 to other IC elements under the following conditions:

a) *General Requirements.* Any dissemination under these Guidelines of any bulk dataset or significant portion of a dataset believed to contain United States person information, which has not been assessed as constituting terrorism information, must be approved by the Director of NCTC and must be expressly allowed by the applicable Terms and Conditions for that dataset or otherwise expressly approved by the data provider. IC elements that receive or access bulk datasets or significant portions of a dataset under these Guidelines are not authorized to make further bulk disseminations of that information.

b) *Bulk Dissemination in Support of Counterterrorism Missions*: The Director of NCTC shall only approve such dissemination to IC elements in support of a legally authorized counterterrorism mission if the receiving element head agrees in writing to abide by the

provisions of the Appendix to these Guidelines and any enhanced safeguards, procedures, and oversight mechanisms identified in the Terms and Conditions for the particular dataset or otherwise required by the Director of NCTC.[4] The agreement must specify, by name or position, the persons responsible for oversight and reporting, consistent with these Guidelines. The ODNI General Counsel and the ODNI Civil Liberties Protection Officer, in consultation with the Assistant Attorney General for National Security, shall verify that the receiving IC element has the capabilities and technology in place to accomplish the necessary oversight and compliance.

c) *Bulk Dissemination in Support of Other Intelligence Missions*: The Director of National Intelligence shall only approve such dissemination to IC elements in support of lawful intelligence missions other than counterterrorism missions if: such dissemination is expressly allowed by the applicable Terms and Conditions; the receiving element has Attorney General-approved procedures in place for the collection, retention, and dissemination of United States person information, as required by the opening paragraph of section 2.3 of Executive Order 12333; and the receiving element head agrees in writing to abide by safeguards, procedures, and oversight mechanisms substantially similar to the safeguards, procedures, and oversight mechanisms identified in the Appendix to these Guidelines, as well as any enhanced safeguards, procedures, and oversight mechanisms identified in the Terms and Conditions for the particular datasets or otherwise required by the Director of NCTC. In addition, the Director of National Intelligence may only approve bulk dissemination to IC elements in support of intelligence missions other than counterterrorism missions if the Director of National Intelligence, in consultation with the ODNI General Counsel, determines that the proposed dissemination is necessary to a lawful mission of the IC element and that the IC element's need for the information cannot be fulfilled through dissemination of specific information under the standard dissemination provisions of section IV.C.1; through dissemination of a smaller portion of the data proposed for dissemination; or by allowing access to the data while it remains within NCTC's control. The Director of National Intelligence will provide a copy of this determination to the Assistant Attorney General for National Security. The agreement must specify, by name or position, the persons responsible for oversight and reporting, consistent with these Guidelines. The ODNI General Counsel and the ODNI Civil Liberties Protection Officer shall verify that the receiving IC element has the capabilities and technology in place to accomplish the necessary oversight and compliance. Any such agreement must be approved by the Attorney General or his delegee prior to allowing such dissemination, and the National Security Division of the Department of Justice may conduct an independent assessment of the element's oversight and compliance capabilities.

[4] If an IC element with a counterterrorism mission requests changes to provisions in the Appendix to address agency-specific circumstances (e.g., technological capabilities), such changes may be adopted if expressly approved by the data provider and by the DNI and the Attorney General or their delegees, provided that any agency-specific Appendix shall retain safeguards, procedures, and oversight mechanisms substantially similar to those contained in the original Appendix.

D. Foreign Disseminations

For any dissemination of United States person information to a foreign or international entity, in addition to complying with the dissemination provisions of section IV, NCTC must find that: (i) the dissemination is consistent with the interests of the United States, including U.S. national security interests; (ii) the dissemination complies with DCID 6/6 or any successor ICD[5]; (iii) the foreign or international entity agrees not to disseminate the information further without approval by NCTC; and (iv) NCTC, in consultation with ODNI General Counsel, has considered the effect such dissemination may reasonably be expected to have on any identifiable United States person to determine whether any additional safeguards are needed.

E. Other Disseminations

If NCTC properly acquires any United States person information under Tracks 1 and 2 that would be authorized for dissemination pursuant to section IV.C.1 if it were acquired under Track 3, it shall consult with the data provider and advise the data provider of the existence of such information. The data provider may disseminate the information or authorize NCTC to do so.

V. Retention of Information for Administrative Purposes

To the extent consistent with law, United States person information acquired pursuant to these Guidelines may be retained if necessary to conduct the oversight, auditing, redress, or compliance activities required by these Guidelines, if required by law or court order to be retained, or if necessary to determine whether the requirements of these Guidelines or applicable laws are satisfied. Any information retained under this paragraph beyond the temporary retention period may not be used for purposes other than those specified in the preceding sentence and must be promptly removed from NCTC's systems once retention is no longer necessary or required for those purposes, except that NCTC may retain any oversight, audit, redress, or compliance records or reports in accordance with its records retention policies.

VI. Compliance

A. Periodic Compliance Reviews

Subject to oversight by the ODNI Civil Liberties Protection Officer, NCTC shall conduct periodic reviews to verify continued compliance with these Guidelines, including compliance with the Terms and Conditions, and with all baseline and enhanced safeguards, procedures, and oversight mechanisms. These reviews shall include spot checks, reviews of audit logs, and other appropriate measures.

[5] ICD 403 is currently in draft. Once signed, any foreign dissemination would be required to comply with ICD 403 and any implementing ICPGs and IC Standards.

B. Periodic Reviews of the Need for Continued Assessment

NCTC, in coordination with the ODNI Civil Liberties Protection Officer, shall conduct periodic reviews of all datasets replicated under Track 3 to determine whether retention and continued assessment of the United States person information in those datasets remains appropriate. In conducting this review, consideration shall be given to the purpose for which the dataset was acquired, the success of that dataset in fulfilling legitimate counterterrorism purposes, whether those purposes can now be fulfilled through Track 1 or 2 access to the dataset, through the use of other datasets in NCTC's possession, or through other appropriate means, and privacy and civil liberties considerations applicable to the particular dataset. NCTC shall also conduct periodic reviews of the continued necessity and efficacy of bulk disseminations permitted under the Guidelines. NCTC shall report the results of these periodic reviews to the IC Inspector General.

C. NCTC's Computer Systems

In designing its computer systems, NCTC shall take reasonable steps to enhance its ability to monitor activity involving United States person information and other sensitive information, and to facilitate compliance with, and the auditing and reporting required by, these Guidelines.

D. Reporting

1. NCTC shall promptly report, in writing, to the Director of NCTC, the ODNI General Counsel, the ODNI Civil Liberties Protection Officer, the Department of Justice, and the IC Inspector General upon discovery of any significant failure to comply with: (i) these Guidelines; (ii) baseline or enhanced safeguards, procedures, or other oversight mechanisms; or (iii) any Terms and Conditions. For the purposes of these Guidelines, a "significant failure" is a failure that constitutes a violation of the Constitution or other law, including any executive order, and/or a failure that leads to unauthorized access, use, or dissemination of personally identifiable information about a United States person. NCTC shall report to any data provider whose information was affected by the noncompliance, in accordance with the Terms and Conditions for that data.

2. The Director of NCTC shall report annually in writing to the ODNI Civil Liberties Protection Officer on the measures that NCTC is taking to ensure that its access to, and retention, use, and dissemination of, United States person information is appropriate under these Guidelines and in compliance with the baseline and enhanced safeguards, procedures, and oversight mechanisms, and all applicable Terms and Conditions. The report shall include:

(1) For datasets replicated under Track 3, the results of the review required in section VI.B above, regarding whether replication continues to be appropriate;

(2) A general description of NCTC's compliance and audit processes;

(3) A description of the audits, spot checks, and other reviews NCTC conducted during the previous year, and the results of those audits, spot checks, or other reviews, to include any shortcomings identified;

(4) A description of how NCTC ensures that it promptly purges United States person information that does not meet the standards for retention under these Guidelines;

(5) An assessment of United States person information disseminated by NCTC directly to foreign, international, state, local, tribal, or private sector entities or individuals; the restrictions, if any, that NCTC imposed on the entities' use or further dissemination of such information; and any known misuse of such information by a recipient, data breach, or significant failure by the recipient to comply with the terms of the certification required under section IV.B.2;

(6) A description of any approvals by the DNI or Director of NCTC, in accordance with sections IV.B.2 and IV.C.2 above, to provide access to or to disseminate bulk datasets or significant portions of a dataset;

(7) An assessment of whether there is a need for enhanced safeguards, procedures, or oversight regarding the handling of United States person information or other sensitive information, or whether any other reasonable measures that should be taken to improve the handling of information;

(8) A description of measures that NCTC has taken to comply with the requirements of section VI.C with respect to its data processing systems; and

(9) A description of any material changes or improvements NCTC implemented, or is considering implementing, to improve compliance with these Guidelines.

3. NCTC shall provide a copy of this report to the ODNI General Counsel and the IC Inspector General, and shall make the report available upon request to the Assistant Attorney General for National Security. NCTC shall also make available to the IC Inspector General any other reports or documentation necessary to ensure compliance with these Guidelines.

4. The reporting required by these Guidelines does not replace any other reporting required by statute, executive order, or regulation.

E. Privacy and Civil Liberties Oversight Board

Pursuant to section 1061 of the Intelligence Reform and Terrorism Prevention Act of 2004, the Privacy and Civil Liberties Oversight Board shall have access to all relevant NCTC records, reports, audits, reviews, documents, papers, recommendations, and other material that it deems relevant to its oversight of NCTC activities.

VII. Interpretation and Departures

A. NCTC shall refer all questions relating to the interpretation of these Guidelines to the ODNI Office of General Counsel. The ODNI General Counsel shall consult with the Assistant Attorney General for National Security regarding any novel or significant interpretations.

B. The ODNI General Counsel and the Assistant Attorney General for National Security must approve any departures from these Guidelines. If there is not time for such approval and a departure from these Guidelines is necessary because of the immediacy or gravity of a threat to the safety of persons or property or to the national security, the Director of NCTC or the Director's senior representative present may approve a departure from these Guidelines. The ODNI General Counsel shall be notified as soon thereafter as possible. The ODNI General Counsel shall provide prompt written notice of any such departures to the Assistant Attorney General for National Security. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States.

VIII. Status as Internal Guidance

These Guidelines are set forth solely for the purpose of internal NCTC and ODNI guidance. They are not intended to, and do not, create any rights, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies, or entities, its officers, employees, agents, or any other person, nor do they place any limitation on otherwise lawful investigative or litigation prerogatives of the United States.

IX. Revocations, Transitions, and Effective Date.

These Guidelines supersede and revoke the Memorandum of Agreement signed by the Director of National Intelligence and Attorney General on October 1, 2008 and November 4, 2008, respectively, along with any amendments to that Agreement. Terms and Conditions entered pursuant to that Memorandum of Agreement, or similar information sharing agreements to which NCTC is currently a party, remain in effect until revoked or until amended or replaced consistent with these Guidelines. As applied to NCTC, these Guidelines also supersede NCTC's EO 12333, § 2.3 Procedures with respect to the data and datasets covered by these Guidelines. These Guidelines shall be effective upon the approval of the Attorney General, the Director of National Intelligence, and the Director of NCTC.

Signed

Matthew G. Olsen

MAR 21 2012

Matthew G. Olsen
Director, National Counterterrorism Center

Date

James R. Clapper

21 MAR 2012

James R. Clapper, Jr.
Director of National Intelligence

Date

3-22-12

Eric H. Holder, Jr.
Attorney General of the United States of America

Date

Appendix

Safeguards, Procedures, and Oversight Mechanisms for Bulk Dissemination of Information Acquired Under Track 3 to IC Elements

I. Purpose

This Appendix contains the safeguards, procedures, and oversight mechanisms that an Intelligence Community (IC) element head, or designee, must agree to, in writing, before NCTC may disseminate any bulk dataset or significant portion of a dataset (hereinafter referred to in this Appendix as "a dataset" or "data") that includes United States Person information in accordance with section IV.C.2(b) of the NCTC Guidelines. NCTC may only disseminate datasets under this Appendix in support of the receiving IC element's legally authorized counterterrorism mission.

II. Implementation

Prior to NCTC's dissemination of any bulk dataset to an IC element, the element head must agree in writing to abide by the provisions of this Appendix, and any enhanced safeguards, procedures, and oversight mechanisms identified in the Terms and Conditions for the particular dataset or otherwise required by the Director of NCTC (hereinafter "written agreement"). All requirements shall be described, referenced, or appended to the written agreement, which the Director of NCTC shall develop in consultation with the ODNI General Counsel and Civil Liberties Protection Officer. If an IC element is provided access to NCTC's systems in support of its legally authorized counterterrorism mission and NCTC will undertake any of the requirements in this Appendix on behalf of the IC element, the IC element head and the Director of NCTC shall specify in the written agreement the persons, by name or position, responsible for all training, oversight, and related compliance measures and reporting.

III. Definitions

For the purposes of this Appendix, the following definitions apply:

A. **Dissemination:** Dissemination means transmitting, communicating, sharing, passing, or providing access to information outside NCTC and/or the IC element by any means, to include oral, electronic, or physical means.

B. **IC Element:** The term "IC element" refers to the specific IC element that is provided data in accordance with section IV.C.2(b) of the NCTC Guidelines in support of the IC element's legally authorized counterterrorism mission.

C. **Terrorism Information:** The term "terrorism information"—

(1) means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to—

(i) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism;
(ii) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;
(iii) communications of or by such groups or individuals; or
(iv) groups or individuals reasonably believed to be assisting or associated with such groups or individuals; and

(2) includes weapons of mass destruction information. 6 U.S.C. § 485(a)(5).

D. United States Person. For an IC element receiving information under this Appendix, this term has the meaning given the term in that element's guidelines approved by the Attorney General under section 2.3 of Executive Order 12333. For an element without such Attorney General-approved guidelines, or whose guidelines do not contain such a definition, this term means a United States citizen, an alien known by the intelligence element concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. *See* Executive Order 12333 § 3.5(k).

IV. General Provisions

A. Authorized Purpose. The IC element may access and acquire United States person information in the dataset for the purpose of determining whether the information is reasonably believed to constitute terrorism information and thus may be permanently retained,[1] used, and disseminated. Any United States person information acquired must be reviewed for such purpose in accordance with the procedures in this Appendix, the applicable Terms and Conditions for that dataset, and any other measures specified in the written agreement. Information is "reasonably believed to constitute terrorism information" if, based on the knowledge and experience of counterterrorism analysts as well as the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the information is terrorism information.

B. Erroneously Provided Information and Errors in Information. Any United States person information that has been erroneously disseminated to the IC element will not be retained, used, or further disseminated by the IC element. Such information will be promptly removed from the IC element's systems, unless such removal is otherwise prohibited by applicable law or court order or by regulation or policy approved by the

[1] For purposes of this Appendix, "permanently retained" does not mean that the information is retained indefinitely, but rather that it is retained in accordance with the IC element's records retention policies.

Attorney General. Information in the IC element's systems found to contain errors will be promptly corrected to ensure information integrity and accuracy, and NCTC shall be notified of the error promptly.

C. **Removal of Information.** The IC element shall remove from the IC element's systems all identified information concerning United States persons that the IC element does not reasonably believe constitutes terrorism information within five years from the date the data is generally available for assessment by NCTC (or within the time period identified in the written agreement if it specifies a shorter temporary retention period), unless such removal is otherwise prohibited by applicable law or court order or by regulation or policy approved by the Attorney General, or unless the information is retained for administrative purposes as authorized in section VII below.

D. **Training.** The IC element shall ensure that all employees and contractors of the IC element and detailees and assignees to the IC element from other agencies (hereinafter "IC element personnel") provided access to the data under this Appendix will receive training in the use of each dataset to which they will have access to ensure that they use the data only for the IC element's authorized counterterrorism purposes and in accordance with this Appendix and other applicable requirements. The training shall also ensure that they understand the baseline and enhanced safeguards, dissemination restrictions, and other privacy and civil liberties protections they must apply to each dataset. This training shall be in person, whenever practical, and refreshed at least annually. IC element personnel provided access to data under this Appendix will also receive ongoing training to ensure understanding of this Appendix and other applicable agreements and the civil liberties and privacy expectations and requirements involved in the access to and use of the data.

E. **Authorized Uses of Information and Time Periods.** For all datasets or data received pursuant to this Appendix, the IC element will use reasonable measures to identify and mark or tag United States person information contained within those datasets (to the extent not already done so by the data provider and NCTC). Any United States person information accessed or acquired in accordance with this Appendix may be continually assessed for up to five years by IC element personnel to determine whether the United States person information is reasonably believed to constitute terrorism information unless a shorter temporary retention period is specified in the written agreement with NCTC. The written agreement signed by the IC element head or designee shall specify the applicable temporary retention period for the dataset or data as required by the Terms and Conditions or otherwise required by the Director of NCTC. The temporary retention period shall commence when the data is made generally available for access and use by NCTC; the period is not restarted at the time of dissemination to or access by the IC element. United States person information that is reasonably believed to constitute terrorism information may be permanently retained and used for all authorized IC element purposes. These include, but are not limited to: analysis and integration purposes, inclusion in finished analytic products and pieces,

enhancement of records contained within the Terrorist Identities Datamart Environment (TIDE), operational support and planning, and appropriate dissemination to Intelligence Community elements, as well as federal and other counterterrorism partners. Specific provisions on use and dissemination are set forth below. Any additional protections or provisions required by the Terms and Conditions for that dataset or otherwise required by the Director of NCTC must be included in the written agreement signed by the IC element head or designee.

F. Applicable Laws and Policies. The IC element shall access, acquire, retain, use, and disseminate information, including United States person information, (i) pursuant to the relevant standards of Executive Order 12333, as amended; (ii) as consistent with the National Security Act of 1947, as amended; and (iii) as authorized by law or regulations, including applicable privacy laws. This Appendix does not apply to information whose retention, use, and dissemination is governed by court order or court-approved procedures. If the IC element has Attorney General-approved procedures pursuant to section 2.3 of Executive Order 12333, those are hereby superseded as applied to the collection, retention, and dissemination of United States person information in data and datasets governed by this Appendix, except as otherwise specifically provided herein.

G. Limitation. The IC element shall not access, acquire, retain, use, or disseminate United States person information solely for the purpose of monitoring activities protected by the First Amendment or monitoring the lawful exercise of other rights secured by the Constitution or other laws of the United States. IC element personnel who access NCTC's databases will be subject at all times to NCTC's Role-Based Access and Information Sharing Policies, and to additional audit and oversight requirements, as applicable and as specified in the written agreement signed by the IC element head or designee. IC elements may be required to adopt or apply similar role-based access and information sharing policies prior to receiving and storing data from NCTC; any such requirements will be specified in the written agreement signed by the IC element head or designee.

H. Information Access Requests. For information governed by this Appendix, it shall be the responsibility of the data provider who provided the data to NCTC to make determinations regarding the Freedom of Information Act and first-party access under the Privacy Act, and discovery or other requests for such information in any legal proceeding, unless a different arrangement was agreed upon between NCTC and the data provider and specified in the Terms and Conditions or is required by law. Information derived from an operational file exempted from search and review, publication, and disclosure under 5 U.S.C. § 552 in accordance with law shall remain under the control of the data provider and be handled as coordinated in advance with the data provider and as specified in the Terms and Conditions for that information.

I. Baseline Safeguards, Procedures, and Oversight Mechanisms. During the temporary retention period, the IC element shall adhere to the following baseline

safeguards, procedures, and oversight mechanisms for any dataset disseminated by NCTC under this Appendix:

1. The data will be maintained in a secure, restricted-access repository.

2. Access to the data will be limited to those IC element personnel, who: (i) access the data for the purpose authorized in section IV.A; (ii) are acting under, and agree to abide by, the IC element's information sharing and use rules, including this Appendix and the written agreement; (iii) have the requisite security clearance and a need-to-know in the course of their official duties; and (iv) have received the training required by section IV.D.

3. Access to the data will be monitored, recorded, and audited. This includes tracking of logons and logoffs, file and object manipulation and changes, and queries executed, in accordance with audit and monitoring standards applicable to the Intelligence Community. Audit records will be protected against unauthorized access, modifications, and deletion, and will be retained for a sufficient period to enable verification of compliance with the rules applicable to the data for which audit records apply.

4. The IC element's queries or other activities to assess information contained in the data disseminated pursuant to this Appendix shall be designed solely to identify information that is reasonably believed to constitute terrorism information.

5. The IC element shall query the data in a way designed to minimize the review of information concerning United States persons that does not constitute terrorism information. To identify information reasonably believed to constitute terrorism information contained in data disseminated pursuant to this Appendix, the IC element may conduct (i) queries that do not consist of, or do not consist exclusively of, terrorism data points, which are known or suspected terrorist identifiers or other pieces of terrorism information, and (ii) pattern-based queries and analyses. To the extent that these activities constitute "data mining" as that term is defined in the Federal Agency Data Mining Reporting Act of 2007, the IC element shall coordinate with NCTC to ensure proper reporting and to identify which element should report these activities as required by that Act.

6. The IC element will conduct compliance reviews as described below in section IX.

J. Enhanced Safeguards, Procedures, and Oversight Mechanisms. The IC element must also comply with any enhanced safeguards, procedures, and oversight mechanisms identified in the Terms and Conditions for the particular dataset or otherwise required by

the Director of NCTC and specified in the written agreement signed by the IC element head or designee. See NCTC Guidelines, section III.C.3(e).

V. Dissemination of United States Person Information

A. General Dissemination Requirements.

1. *Terms and Conditions and Privacy Act.* All disseminations under this Appendix must be: (i) compatible with this Appendix; (ii) any applicable Terms and Conditions, and any other measures identified or specified in the written agreement or, if not compatible, the data provider must have otherwise consented to the dissemination; and (iii) permissible under the Privacy Act, 5 U.S.C. § 552a, if applicable.

2. *Dissemination to State, Local, or Tribal Authorities or Private-Sector Entities.* The NCTC Guidelines and this Appendix are not intended to alter or otherwise impact pre-existing information sharing relationships by federal agencies with state, local, or tribal authorities or private-sector entities, whether such relationships arise by law, Presidential Directive, MOU, or other formal agreement (including, but not limited to, those listed in section II of the NCTC Guidelines). To the extent that the NCTC Guidelines, this Appendix, and the written agreement allow for dissemination to state, local, tribal, or private sector entities, such dissemination will continue to be made, consistent with section 119(f)(1)(E) of the National Security Act (50 U.S.C. 404o(f)(1)(E)), in support of the Department of Justice (including the FBI) or the Department of Homeland Security responsibilities to disseminate terrorism information to these entities, and conducted under agreements with those Departments. This Appendix is not intended to, does not, and shall not be relied upon to create a grant of new or additional authority for information sharing with or dissemination of information to state, local, or tribal authorities or private-sector entitles.

3. *Bulk Disseminations Prohibited.* In no case may the IC element make a further bulk dissemination of any dataset or any significant portion of a dataset. However, specific United States person information may be disseminated pursuant to the dissemination provisions in sections V.B or V.C below.

B. Basic Dissemination Requirements. The IC element may disseminate United States person information from datasets provided by NCTC if the General Dissemination Requirements are met, and if:

1. *Dissemination of Terrorism Information.* The United States person information reasonably appears to constitute terrorism information, or reasonably appears to be necessary to understand or assess terrorism information, and the IC element is disseminating the information to a federal, state, local, tribal, or foreign or international entity, or to any other appropriate entity or individual, that is

reasonably believed to have a need to receive such information for the performance of a lawful function;

2. *Dissemination for Limited Purposes.* The United States person information is disseminated to other elements of the Intelligence Community or to a federal, state, local, tribal, or foreign or international entity, or to any other appropriate entity, for the limited purpose of assisting the IC element in determining whether the United States person information constitutes terrorism information. Before disseminating information under this paragraph, the IC element should consider approaching NCTC for this type of assistance. Any such recipients may only use the information for the limited purpose identified in this paragraph, and may not use the information for any other purpose or disseminate the information further without the prior approval of NCTC. Recipients of information under this paragraph must promptly provide the requested assistance to the IC element and promptly thereafter return the information to the IC element or destroy it unless the IC element authorizes continued retention after the specific information continued retention after the specific information is determined by the IC element to meet the dissemination criteria in section V.C of this Appendix. Recipients of information under this paragraph may not retain the information for continual assessment of whether it constitutes terrorism information unless such retention is permitted by the dissemination criteria in section V.C of this Appendix. This paragraph does not authorize the IC element to disseminate any bulk dataset or significant portion of a dataset believed to contain United States person information;

3. *Dissemination Based on Consent.* The United States person whom the information concerns consents to the dissemination; or

4. *Dissemination of Publicly Available Information.* The United States person information is publicly available.

C. Dissemination of Non-Terrorism Information. In addition, the IC element may disseminate United States person information contained in datasets provided by NCTC if that United States person information has been handled and subsequently identified in accordance with applicable safeguards and procedures,[2] if the General Dissemination Requirements are met, and if the United States person information:

1. Reasonably appears to be foreign intelligence or counterintelligence, or information concerning foreign aspects of international narcotics activities, or

[2] Note that this dissemination category does not authorize the IC element to search for additional categories of information, but rather allows the IC element to disseminate certain United States person information uncovered while performing counterterrorism analysis and searches in accordance with this Appendix, the applicable Terms and Conditions, and the written agreement.

reasonably appears to be necessary to understand or assess foreign intelligence or counterintelligence or foreign aspects of international narcotics activities, and the IC element is disseminating the information to another federal, state, local, tribal, or foreign or international entity that is reasonably believed to have a need to receive such information for the performance of a lawful function, provided they agree to such further restrictions on dissemination as may be necessary;

2. Reasonably appears to be evidence of a crime, and the IC element is disseminating the information to another federal, state, local, tribal, or foreign agency that is reasonably believed to have jurisdiction or responsibility for the investigation or prosecution to which the information relates and a need to receive such information for the performance of a lawful governmental function;

3. Is disseminated to a Congressional Committee to perform its lawful oversight functions, after approval by the IC element's Office of General Counsel or senior legal advisor;

4. Is disseminated to a federal, state, local, tribal, or foreign or international entity, or to an individual or entity not part of a government, and is reasonably believed to be necessary to: (i) protect the safety or security of persons, property, or organizations; or (ii) protect against or prevent a crime or a threat to the national security, provided they agree to such further restrictions on dissemination as may be necessary;

5. Is disseminated to another federal, state, local, tribal, or foreign or international entity for the purpose of determining the suitability or credibility of persons who are reasonably believed to be potential sources or contacts, provided they agree to such further restrictions on dissemination as may be necessary;

6. Is disseminated to another federal, state, local, tribal, or foreign or international entity for the purpose of protecting foreign intelligence or counterintelligence sources and methods from unauthorized disclosure;

7. Is disseminated to other recipients, if the subject of the information provides prior consent in writing;

8. Is otherwise required to be disseminated by statutes; treaties; executive orders; Presidential directives; National Security Council directives; Homeland Security Council directives; or Attorney General-approved policies, memoranda of understanding, or agreements; or

9. Is disseminated to appropriate elements of the IC for the purposes of allowing the recipient element to determine whether the information is relevant to its responsibilities and can be retained by it.

The identity of a United States person may be disseminated outside the Intelligence Community only if it is necessary or if it is reasonably believed it may become necessary to understand and assess such United States person information described above.

VI. Foreign Disseminations

For any dissemination of United States person information to a foreign or international entity, in addition to complying with the dissemination provisions of section V, the IC element must find that:

A. the dissemination is consistent with the interests of the United States, including U.S. national security interests;

B. the dissemination complies with DCID 6/6 or any successor ICD[3];

C. the foreign or international entity has agreed not to disseminate the information further without approval by the IC element; and

D. the IC element, in consultation with its General Counsel or senior legal advisor, has considered the effect such dissemination may reasonably be expected to have on any identifiable United States person to determine whether any additional safeguards are needed.

VII. Retention of Information for Administrative Purposes

To the extent consistent with law, United States person information acquired pursuant to this Appendix may be retained if necessary to conduct the oversight, auditing, redress, or compliance activities required by these Guidelines, if required by law or court order to be retained, or if necessary to determine whether the requirements of these Guidelines or applicable laws are satisfied. Any information retained under this paragraph beyond the temporary retention period may not be used for purposes other than those specified in the preceding sentence and must be promptly removed from the IC element's systems once retention is no longer necessary or required for those purposes, except that the IC element may retain any oversight, audit, redress, or compliance records or reports in accordance with its records retention policies.

VIII. The IC Element's Computer Systems

In designing its computer systems, the IC element shall take reasonable steps to enhance its ability to monitor activity involving United States person information and other sensitive information, and to facilitate compliance with, and the auditing and reporting required by, this Appendix.

[3] ICD 403 is currently in draft. Once signed, any foreign dissemination would be required to comply with ICD 403 and any implementing IC Policy Guidance and IC Standards.

IX. Oversight and Compliance

A. Subject to oversight by the IC element's Civil Liberties and/or Privacy Officer, if applicable, and the ODNI Civil Liberties Protection Officer, the IC element shall conduct periodic reviews to verify continued compliance with this Appendix, including compliance with any Terms and Conditions and any measures specified in the written agreement. These reviews shall include spot checks, reviews of audit logs, and other appropriate measures.

B. The IC element, in coordination with the IC element's Civil Liberties and/or Privacy Officer (or other appropriate official as identified in the written agreement), shall conduct periodic reviews of its continued need for access to each dataset disseminated pursuant to the NCTC Guidelines and this Appendix to determine whether such access remains necessary and appropriate. In conducting this review, consideration shall be given to the purpose for which the dataset was disseminated; the success of that dataset in fulfilling legitimate counterterrorism purposes; whether those purposes can now be fulfilled through the use of other data in the IC element's possession, or through other appropriate means; and privacy and civil liberties considerations applicable to the particular dataset.

C. The IC element shall promptly report, in writing, to the IC element head, the Director of NCTC, the ODNI General Counsel, the ODNI Civil Liberties Protection Officer, the Department of Justice, and the IC Inspector General upon discovery of any significant failure to comply with (i) this Appendix; (ii) baseline or enhanced safeguards, procedures, or other oversight mechanisms; or (iii) any Terms and Conditions or the written agreement. For the purposes of this Appendix, a "significant failure" is a failure that constitutes a violation of the Constitution, or other law, including any executive order, and/or a failure that leads to unauthorized access, use, or dissemination of personally identifiable information about a United States person. NCTC shall then report to any data provider whose information was affected by the noncompliance, in accordance with the Terms and Conditions for that data.

D. The IC element shall report annually in writing to the IC element head and to the ODNI Civil Liberties Protection Officer on the measures that the IC element is taking to ensure that its access to, and retention, use, and dissemination of, United States person information is appropriate under this Appendix, and in compliance with all Terms and Conditions and written agreement. The report shall include:

1. The results of the review required in section IX.B. above, regarding whether access to the bulk dataset continues to be appropriate;

2. A general description of the IC element's compliance and audit processes;

3. A description of the audits, spot checks, and other reviews the IC element conducted during the previous year, and the results of those audits, spot checks or other reviews, to include any shortcomings identified;

4. A description of how the IC element ensures that it promptly purges United States person information that does not meet the standards for retention under this Appendix, related Terms and Conditions, and any other measures specified in the written agreement;

5. An assessment of the United States person information disseminated by the IC element directly to foreign, international, state, local, tribal, or private sector entities or individuals; the restrictions, if any, that the IC element imposed on the entities' use or further dissemination of such information; and any known misuse of such information by a recipient, data breach, or significant failure by the recipient to comply with the terms of the certification required under section VI.C of this Appendix;

6. An assessment of whether there is a need for enhanced safeguards, procedures, or oversight regarding the handling of United States person information or other sensitive information, or any other reasonable measures that should be taken to improve the handling of information;

7. Measures the IC element has taken to comply with the requirements of section VIII with respect to its computer systems; and

8. A description of any material changes or improvements the IC element implemented, or is considering implementing, to improve compliance with this Appendix.

E. The IC element shall provide a copy of this report to the IC element General Counsel, the IC element Civil Liberties and/or Privacy Officer, the Director of NCTC, the ODNI General Counsel, the IC element's Inspector General, and the IC Inspector General, and shall make the report available upon request to the Assistant Attorney General for National Security. The IC element shall also make available to the IC element's Inspector General and the IC Inspector General any other reports or documentation necessary to ensure compliance with this Appendix.

F. The reporting required by this Appendix does not replace any other reporting required by statute, executive order, or regulation.

X. Interpretation and Departures

A. The IC element shall refer all questions relating to the interpretation of these Guidelines to the IC element's Office of General Counsel or other senior legal advisor. The IC element's General Counsel shall consult with the ODNI General Counsel regarding any novel or significant interpretations, and the ODNI General Counsel shall

then consult with the Assistant Attorney General for National Security to the extent required by the NCTC Guidelines.

B. The ODNI General Counsel and the Assistant Attorney General for National Security must approve in advance any departures from this Appendix. If there is not time for such approval and a departure from this Appendix is necessary because of the immediacy or gravity of a threat to the safety of persons or property or to the national security, the IC element head, other senior IC element personnel identified in the written agreement with NCTC, the Director of NCTC, or the NCTC Director's senior representative present may approve a departure from these Guidelines. The ODNI General Counsel shall be notified as soon thereafter as possible. The ODNI General Counsel shall provide prompt written notice of any such departures to the Assistant Attorney General for National Security. Notwithstanding this paragraph, all activities in all circumstances must be carried out in a manner consistent with the Constitution and laws of the United States.

XI. Status as Internal Guidance

The provisions in this Appendix are set forth solely for the purpose of internal IC element and ODNI guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law or in equity, by any party in any matter, civil or criminal, nor do they place any limitation on otherwise lawful investigative and litigation prerogatives of the U.S. Government.

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE
PART I - CRIMES
CHAPTER 121 - STORED WIRE AND ELECTRONIC COMMUNICATIONS AND TRANSACTIONAL RECORDS ACCESS

§ 2703. Required disclosure of customer communications or records

(a) Contents of Wire or Electronic Communications in Electronic Storage.— A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of Wire or Electronic Communications in a Remote Computing Service.—

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records Concerning Electronic Communication Service or Remote Computing Service.—

(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for Court Order.— A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) No Cause of Action Against a Provider Disclosing Information Under This Chapter.— No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) Requirement To Preserve Evidence.—

(1) In general.— A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention.— Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) Presence of Officer Not Required.— Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

(Added Pub. L. 99–508, title II, § 201[(a)], Oct. 21, 1986, 100 Stat. 1861; amended Pub. L. 100–690, title VII, §§ 7038, 7039, Nov. 18, 1988, 102 Stat. 4399; Pub. L. 103–322, title XXXIII, § 330003(b), Sept. 13, 1994, 108 Stat. 2140; Pub. L. 103–414, title II, § 207(a), Oct. 25, 1994, 108 Stat. 4292; Pub. L. 104–132, title VIII, § 804, Apr. 24, 1996, 110 Stat. 1305; Pub. L. 104–293, title VI, § 601(b), Oct. 11, 1996, 110 Stat. 3469; Pub. L. 104–294, title VI, § 605(f), Oct. 11, 1996, 110 Stat. 3510; Pub. L. 105–184, § 8, June 23, 1998, 112 Stat. 522; Pub. L. 107–56, title II, §§ 209(2), 210, 212 (b)(1), 220 (a)(1), (b), Oct. 26, 2001, 115 Stat. 283, 285, 291, 292; Pub. L. 107–273, div. B, title IV, § 4005(a)(2), div. C, title I, § 11010, Nov. 2, 2002, 116 Stat. 1812, 1822; Pub. L. 107–296, title II, § 225(h)(1), Nov. 25, 2002, 116 Stat. 2158; Pub. L. 109–162, title XI, § 1171(a)(1), Jan. 5, 2006, 119 Stat. 3123; Pub. L. 111–79, § 2(1), Oct. 19, 2009, 123 Stat. 2086.)

References in Text

The Federal Rules of Criminal Procedure, referred to in subsecs. (a), (b)(1)(A), and (c)(1)(B)(i), are set out in the Appendix to this title.

Amendments

2009—Subsecs. (a), (b)(1)(A), (c)(1)(A). Pub. L. 111–79, which directed substitution of "(or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction" for "by a court with jurisdiction over the offense under investigation or an equivalent State warrant", was executed by making the substitution for "by a court with jurisdiction over the offense under investigation or equivalent State warrant" to reflect the probable intent of Congress.

2006—Subsec. (c)(1)(C). Pub. L. 109–162 struck out "or" at end.

2002—Subsec. (c)(1)(E). Pub. L. 107–273, § 4005(a)(2), realigned margins.

Subsec. (e). Pub. L. 107–296 inserted ", statutory authorization" after "subpoena".

Subsec. (g). Pub. L. 107–273, § 11010, added subsec. (g).

2001—Pub. L. 107–56, § 212(b)(1)(A), substituted "Required disclosure of customer communications or records" for "Requirements for governmental access" in section catchline.

Subsec. (a). Pub. L. 107–56, §§ 209(2)(A), (B), 220 (a)(1), substituted "Contents of Wire or Electronic" for "Contents of Electronic" in heading and "contents of a wire or electronic" for "contents of an electronic" in two places and "using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation" for "under the Federal Rules of Criminal Procedure" in text.

Subsec. (b). Pub. L. 107–56, § 209(2)(A), substituted "Contents of Wire or Electronic" for "Contents of Electronic" in heading.

Subsec. (b)(1). Pub. L. 107–56, §§ 209(2)(C), 220 (a)(1), substituted "any wire or electronic communication" for "any electronic communication" in introductory provisions and "using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation" for "under the Federal Rules of Criminal Procedure" in subpar. (A).

Subsec. (b)(2). Pub. L. 107–56, § 209(2)(C), substituted "any wire or electronic communication" for "any electronic communication" in introductory provisions.

Subsec. (c)(1). Pub. L. 107–56, §§ 212(b)(1)(C), 220 (a)(1), designated subpar. (A) and introductory provisions of subpar. (B) as par. (1), substituted "A governmental entity may require a provider of electronic communication service or remote computing service to" for "(A) Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may" and a closing parenthesis for provisions which began with "covered by subsection (a) or (b) of this section) to any person other than a governmental entity." in former subpar. (A) and ended with "(B) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity", redesignated clauses (i) to (iv) of former subpar. (B) as subpars. (A) to (D), respectively, substituted "using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation" for "under the Federal Rules of Criminal Procedure" in subpar. (A) and "; or" for period at end of subpar. (D), added subpar. (E), and redesignated former subpar. (C) as par. (2).

Subsec. (c)(2). Pub. L. 107–56, § 210, amended par. (2), as redesignated by section 212 of Pub. L. 107–56, by substituting "entity the—" for "entity the name, address, local and long distance telephone toll billing records,

telephone number or other subscriber number or identity, and length of service of a subscriber" in introductory provisions, inserting subpars. (A) to (F), striking out "and the types of services the subscriber or customer utilized," before "when the governmental entity uses an administrative subpoena", inserting "of a subscriber" at beginning of concluding provisions and designating "to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1)." as remainder of concluding provisions.

Pub. L. 107–56, § 212(b)(1)(C)(iii), (D), redesignated subpar. (C) of par. (1) as par. (2) and temporarily substituted "paragraph (1)" for "subparagraph (B)".

Pub. L. 107–56, § 212(b)(1)(B), redesignated par. (2) as (3).

Subsec. (c)(3). Pub. L. 107–56, § 212(b)(1)(B), redesignated par. (2) as (3).

Subsec. (d). Pub. L. 107–56, § 220(b), struck out "described in section 3127 (2)(A)" after "court of competent jurisdiction".

1998—Subsec. (c)(1)(B)(iv). Pub. L. 105–184 added cl. (iv).

1996—Subsec. (c)(1)(C). Pub. L. 104–293 inserted "local and long distance" after "address,".

Subsec. (d). Pub. L. 104–294 substituted "in section 3127 (2)(A)" for "in section 3126 (2)(A)".

Subsec. (f). Pub. L. 104–132 added subsec. (f).

1994—Subsec. (c)(1)(B). Pub. L. 103–414, § 207(a)(1)(A), redesignated cls. (ii) to (iv) as (i) to (iii), respectively, and struck out former cl. (i) which read as follows: "uses an administrative subpoena authorized by a Federal or State statute, or a Federal or State grand jury or trial subpoena;".

Subsec. (c)(1)(C). Pub. L. 103–414, § 207(a)(1)(B), added subpar. (C).

Subsec. (d). Pub. L. 103–414, § 207(a)(2), amended first sentence generally. Prior to amendment, first sentence read as follows: "A court order for disclosure under subsection (b) or (c) of this section may be issued by any court that is a court of competent jurisdiction set forth in section 3127 (2)(A) of this title and shall issue only if the governmental entity shows that there is reason to believe the contents of a wire or electronic communication, or the records or other information sought, are relevant to a legitimate law enforcement inquiry."

Pub. L. 103–322 substituted "section 3127 (2)(A)" for "section 3126 (2)(A)".

1988—Subsecs. (b)(1)(B)(i), (c)(1)(B)(i). Pub. L. 100–690, § 7038, inserted "or trial" after "grand jury".

Subsec. (d). Pub. L. 100–690, § 7039, inserted "may be issued by any court that is a court of competent jurisdiction set forth in section 3126 (2)(A) of this title and" before "shall issue".

Effective Date of 2002 Amendment

Amendment by Pub. L. 107–296 effective 60 days after Nov. 25, 2002, see section 4 of Pub. L. 107–296, set out as an Effective Date note under section 101 of Title 6, Domestic Security.

The Electronic Communications Privacy Act of 1986: Principles for Reform

J. Beckwith Burr[1]

Background

Congressional enactment of the Electronic Privacy Information Act (ECPA)[2/] in 1986 was a remarkably forward-looking effort to govern the compelled disclosure of electronic communications data to the government by balancing law enforcement needs with the personal privacy safeguards needed in the digital age.[3/] As communications technology developed, and its contribution to the U.S. economy became clear, Congress also consciously endeavored to find a balance that would nurture communications technologies.[4/] The wisdom of this attempt to balance privacy rights and law enforcement needs in an innovation-friendly environment is evident today: the Internet has evolved from a research network with a few thousand academic hosts into a global platform for communications, commerce, and civic activity used by four out of five adults in the United States on a daily basis.[5/] Information technology has driven the U.S.

---

1 J. Beckwith Burr is a partner at Wilmer Cutler Pickering Hale and Dorr, LLP, and a member of the firm's Regulatory and Government Affairs Department, based in Washington, D.C.

2/ The term "ECPA" is used in this paper to describe both Title I of the Electronic Communications Privacy Act, which protects wire, oral, and electronic communications in transit, as well as Title II, referred to as the Stored Communications Act, which protects communication held in electronic storage.

3/ The stated goal of ECPA was to preserve "a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement." House Committee on the Judiciary, Electronic Communications Privacy Act of 1986, H. Rep. No. 99-647, 99th Cong. 2d Sess. 2, at 19 (1986).

4/ In addition to the goals of privacy and law enforcement, ECPA sought to advance the goal of supporting the development and use of these new technologies and services. *See* S. Rep. No. 99-541, at 5 (noting that legal uncertainty over the privacy status of new forms of communications "may unnecessarily discourage potential customers from using innovative communications systems"). It was the intent of Congress to encourage the proliferation of new communications technologies, but it recognized that consumers would not trust new technologies if the privacy of those using them was not protected. *Id.*; H.R. Rep. No. 99-647, at 19 (1986).

5/ Pew Internet & American Life Project: *Wireless Internet Use*, at 8 (July 2009) , *available at* http://www.pewinternet.org/~/media//Files/Reports/2009/Wireless-Internet-Use.pdf

economy in the past two decades,[6/] and is expected to remain the engine of growth for years to come.[7/]

As forward-looking as ECPA was in 1986, there is broad consensus that today's technology has outpaced the Act. In 1983, Apple Computer introduced the "Lisa"—the first mass-marketed microcomputer with a graphical user interface. The Lisa cost $10,000 and featured 1 megabyte of RAM and a 5 megabyte hard drive.[8/] Today, for $999, consumers can purchase a Mac Book with 2 gigabytes of memory, a 250 gigabyte hard drive, and built in wireless Internet access and communications technology.[9/] In 1995—nearly a decade *after* Congress enacted ECPA—only 9% of American adults used the Internet, compared to 81% today.[10/] Prototype mobile telephones from the 1980s—the size and shape of "bricks"—are now

---

6/ *See* Robert D. Atkinson & Andrew S. McKay, *Information Technology & Innovation Foundation, Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution* at 11-14 (March 2007) ("[T]he mid-1990s were a turning point that marked the move from the sluggish U.S. economy of the 1970s, 1980s, and early 1990s to the dynamo of the last decade… [T]here is a now a strong consensus among economists that the IT revolution was and continues to be responsible for the lion's share of the post '95 rebound in productivity growth.").

7/ *See id.* at 53 ("It is not clear how long IT will power growth, but it seems likely that for a[t] least the next decade or two IT will remain the engine of growth. The opportunities for continued diffusion and growth of the IT system appear to be strong. Many sectors, such as health care, education, and government, have only begun to tap the benefits of IT-driven transformation. Adoption rates of e-commerce for most consumers, while rapid, are still relatively low. And new technologies (*e.g.*, RFID, wireless broadband, voice recognition) keep emerging that will enable new applications. In short, while the emerging digital economy has produced enormous benefits, the best is yet to come. The job of policymakers in developed and developing nations alike, is to ensure that the policies and programs they put in place spur digital transformation so that all their citizens can fully benefit from robust rates of growth.").

According to the Bureau of Labor Statistics, "Two of the fastest growing detailed occupations are in the computer specialist occupational group. Network systems and data communications analysts are projected to be the second-fastest-growing occupation in the economy. Demand for these workers will increase as organizations continue to upgrade their information technology capacity and incorporate the newest technologies. The growing reliance on wireless networks will result in a need for more network systems and data communications analysts as well. Computer applications software engineers also are expected to grow rapidly from 2008 to 2018. Expanding Internet technologies have spurred demand for these workers, who can develop Internet, intranet, and Web applications." *Occupational Outlook Handbook: 2010-2011 Edition, available at* http://www.bls.gov/oco/oco2003.htm.

8/ Lisa/Lisa 2/Mac XL, *available at* http://www.apple-history.com/lisa.html.

9/ Apple—MacBook: Technical Specifications, *available at* http://www.apple.com/macbook/specs.html (last visited Feb 2010).

10/ Harris Interactive, The Harris Poll, *available at* http://www.harrisinteractive.com/harris_poll/index.asp?PID=973.

collector's items on eBay,[11/] while in 2009 palm-sized smart phones[12/] double as sophisticated computing platforms with the potential to bridge the digital divide.[13/] Communications technology in the United States is evolving—and will continue to evolve—more rapidly and in more directions than we currently imagine. ECPA, which served us remarkably well for many years, is today unwieldy and unreliable as a law enforcement tool, immensely difficult for judges and investigators to apply, confusing, costly, and full of legal uncertainty for communications and other technology tools and service providers, and an unpredictable guardian of our country's long cherished privacy values.

A coalition of communications, equipment, and online services, as well as members of the legal and advocacy communities[14/] have come together over the last year with the goal of developing a set of principles to simplify, clarify, and unify ECPA—without constraining important law enforcement activities. The result of this effort is a set of consensus principles for updating ECPA that are designed to:

- **Establish consistent, predictable privacy protections** for communications and other electronic information services used by Americans every day to handle their personal communications and operate their businesses — building user trust and supporting the full extension of Constitutional values to the networked world, while providing clarity for law enforcement and service providers.

- **Achieve technologically neutral solutions** and avoid arbitrary distinctions that become hard to apply over time, inhibit innovation, and skew the Internet marketplace.

11/ For example, Motorola's Dynatax 8000x was the first cell phone to receive FCC approval (in 1983). It weighed 28 ounces and was 10 inches high, not including its flexible "rubber duck" whip antenna. *Available at* http://www.retrowow.co.uk/retro_collectibles/80s/motorola_8000X.php.

12/ For example, the Google Nexus One is less than 5 inches tall and weighs less than 5 ounces. *Available at* http://www.google.com/phone/static/en_US-nexusone_tech_specs.html.

13/ According to the Pew Internet & American Life Project, lower levels of home broadband access coupled with lower levels of desktop and laptop computers explains the traditional access gap between white and black Americans. But the gap in online engagement "largely dissipates" according to Pew, when access on handheld and mobile devices is considered: under those circumstances, "use among African Americans matches or exceeds that of white Americans. Two measures of engagement with the wireless online—accessing the [I]nternet on a handheld on the typical day or ever—shows that Africans Americans are *70% more likely* to do this than white Americans." The report concludes, "To an extent notably greater than that for whites, wireless access for African Americans serves as a substitute for a missing onramp to the Internet—the home broadband connection." Pew Internet & American Life Project: *Wireless Internet Use*, at 32-35 (July 2009), *available at* http://www.pewinternet.org/~/media//Files/Reports/2009/Wireless-Internet-Use.pdf (emphasis in original).

14/ Coalition members currently include: American Civil Liberties Union, AT&T, Center for Democracy and Technology, Electronic Frontier Foundation, Google, Microsoft, IBM, Net Coalition, Loopt, and Salesforce.com.

- **Preserve the legal tools necessary to conduct criminal investigations and protect the public**, including through preservation of the ECPA exceptions and exemptions relied upon by law enforcement today.

The consensus principles reflect the working group's commitment to *change no more than strictly necessary to achieve these important goals*. Implementation of the consensus principles would not affect surveillance or privacy law relating to national security, including the Foreign Intelligence Surveillance Act and the national security letter authority in ECPA. The principles would not deny the government information needed to conduct investigations, and no information would be rendered off limits to government investigators with appropriate process. Indeed, adoption of the principles would facilitate cooperation between business and law enforcement by clarifying the rules under which the parties interact. The principles preserve all of the building blocks of criminal investigations—subpoenas, court orders, pen register/trap and trace orders, and warrants, and would carry forward ECPA's sliding scale approach that ties the level of process required to the level of investigative intrusiveness. The recommended changes would not disturb fundamental elements of ECPA, including the distinctions between content, subscriber identifying information, and less sensitive transactional data. Finally, these recommendations preserve the exceptions for compelled disclosure that have been written into ECPA over the years, including those permitting emergency disclosures.

Principles

1. A governmental entity may require an entity covered by ECPA (a provider of wire or electronic communication service or a provider of remote computing service) to disclose communications that are not readily accessible to the public only with a search warrant issued based on a showing of probable cause, regardless of the age of the communications, the means or status of their storage or the provider's access to or use of the communications in its normal business operations.

2. A governmental entity may access, or may require a covered entity to provide, prospectively or retrospectively, location information regarding a mobile communications device only with a warrant issued based on a showing of probable cause.

3. A governmental entity may access, or may require a covered entity to provide, prospectively or in real time, dialed number information, email to and from information or other data currently covered by the authority for pen registers and trap and trace devices only after judicial review and a court finding that the governmental entity has made a showing at least as strong as the showing under 2703(d).

4. Where the Stored Communications Act authorizes a subpoena to acquire information, a governmental entity may use such subpoenas only for information related to a specified account(s) or individual(s). All non-particularized requests must be subject to judicial approval.

Principle 1: Access to Content in Transit and in Storage

Recommended Approach: Under the consensus principles, a governmental entity may require the provider of wire or electronic communications services to produce the non-public content of communications only with a search warrant issued based on a showing of probable cause, regardless of the age of the communication, the means or status of its storage or the provider's access to or use of the content in its business operations. This change would bring all stored communications content under the same probable cause standard set forth in the Fourth Amendment, accessible to law enforcement with an ordinary warrant. For example, a showing of probable cause would be required to compel production of email, regardless of whether it is "opened" or not, and regardless of how old it is. The principle also would apply to documents and other private data stored by or on behalf of individuals on remote servers.[15/]

Need for Change: Americans have embraced email in their professional and personal lives and use it daily for confidential communications of a personal or business nature. Most people save these emails, just as they previously saved letters and other correspondence.[16/] In fact, many Americans now have accumulated years' worth of email, much of which is stored on the computers of trusted third-party service providers. Likewise, businesses and individuals are

---

15/ These changes are premised on the understanding that the definition of "electronic communications" is broad enough to include such items as a draft document stored on a service such as Google Docs. We interpret the current definition of remote computing service as broad enough that it does not need to be amended to cover technologies such as cloud computing, which are expected to keep America competitive by reducing business costs, enhancing productivity, and facilitating collaboration and innovation.

16/ Companies often impose email retention policies that require employees to preserve emails for several months before deletion. Contoural White Paper, *How Long Should Email Be Saved?*, at 5 (2007), *available at* http://www.umiacs.umd.edu/~oard/teaching/708x/spring09/t1.pdf. ("Most companies come to the conclusion that many messages should be retained for a few years for business productivity purposes.").

Moreover, unlike a paper letter, often an email remains in existence long after the sender or recipient attempts to delete it. *See* Applied Discovery, at 3, *available at* http://www2.acc/chapters/program/dallas/documentretention.pdf. ("Even when a computer user intends to discard electronic data, the task is much easier said than done. The 'delete' key creates a false sense of security for many people. A deleted document may no longer be available to the user, but copies remain in temporary files, on backup tapes, and, in the case of email, in other recipients' in-boxes.")

now increasingly storing other data "in the cloud,"[17] with huge benefits in terms of productivity, cost, security, flexibility and the ability to work with collaborators around the world.[18] This data includes highly personal information such as medical and financial data, digital calendars, photographs, diaries, and correspondence.[19] It also includes commercially sensitive, proprietary and trade secret materials, such as business plans, research and development, and commercial collaboration.

The privacy rights of an individual with respect to all of this information, if stored on his or her hard-drive[20]—or indeed on a CD in a safe deposit box—would be fully protected by the warrant clause.[21] Under ECPA, however, a single email or electronic document could be subject to multiple legal standards in its lifecycle, from the moment it is being typed to the moment it is opened by the recipient or uploaded into a user's "vault" in the cloud, where it might be subject to an entirely different standard.[22] A warrant is required to access the content

---

17 "Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The name cloud computing was inspired by the cloud symbol that's often used to represent the Internet in flow charts and diagrams." Cloud Computing Definition, *available at* http://searchcloudcomputing.techtarget.com/sDefinition/0,,sid201_gci1287881,00.html.

18 As an example of the potential savings from cloud computing, the Obama Administration's Chief Information Officer, Vivek Kundra, "pointed to a revamping of the General Services Administration's USA.gov site. Using a traditional approach to add scalability and flexibility, he said, it would have taken six months and cost the government $2.5 million a year. But by turning to a cloud computing approach, the upgrade took just a day and cost $800,000 a year." Daniel Terdiman *White House Unveils Cloud Computing Initiative*, cnet News, Sept. 15, 2009, *available at* http://news.cnet.com/8301-13772_3-10353479-52.html

19 These materials are, as one author has noted, "the same materials deemed 'highly personal' by the Supreme Court, a sentiment later echoed by the Eighth Circuit to justify Fourth Amendment protection for schoolchildren despite their otherwise diminished expectations of privacy. [They] also mirror [ ] the list of materials that the Eleventh Circuit used as a basis for asserting that 'few places outside one's home justify a greater expectation of privacy than does the briefcase.'" *See* David A. Couillard , *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 Minn. L. Rev. 2205, 2219-2220 (2009) (internal footnotes omitted).

20 *See, e.g.*, *Trulock v. Freeh*, 275 F.3d 391 (4th Cir. 2001); *United States v. Crist*, No. 1:07-cr-211, 2008 WL 4682806 (M.D. Pa. Oct. 22, 2008).

21 See, *e.g.*, *Kyllo v. United States,* 533 U.S. 27, 31 (2001) ("At the very core of the Fourth Amendment stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion. With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no." (internal quotations and citations omitted)).

22 Robert Gellman, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, at 13 (Feb. 23, 2009). "Distinctions recognized by ECPA include electronic mail in transit; electronic mail in storage for less than or more than 180 days; electronic mail in draft; opened vs. unopened electronic mail; electronic communication service; and remote computing service.... The precise characterization of an activity can make a significant difference to the protections afforded under ECPA." *Available at* http://www.scribd.com/doc/12805751/Privacy-in-Cloud-Computing-World-Privacy-Council-Feb-2009.

of an email while it is in storage waiting to be read by the recipient.[23] The nanosecond the email is opened by the recipient, however, it may lose that high standard of protection and become accessible with a subpoena, issued with no judicial intervention, with (concurrent or delayed) notice to the affected individual.[24] One Court of Appeals has rejected this distinction between opened and unopened communications for purposes of determining whether or not a communication is in "electronic storage,"[25] while in other areas of the country the question remains unsettled.[26] In all cases, the Justice Department believes law enforcement can compel disclosure of the content of the same email with a mere subpoena after the email is more than

---

[23] 18 U.S.C. § 2703(a).

[24] 18 U.S.C. § 2703(b)(1)(B). Alternatively, it can be acquired with prior notice to the subscriber based upon a court order supported by specific and articulable facts demonstrating reasonable grounds to believe the communication is relevant to an ongoing criminal investigation. *Id.* In either case, notice to the subscriber is required unless the government secures a warrant. *Id.* The Department of Justice Computer Crimes and Intellectual Property Section argues in the 2009 edition of its Computer Search and Seizure Manual, at 123-124: "As traditionally understood, 'electronic storage' refers only to temporary storage made in the course of transmission by a service provider and to backups of such intermediate communications made by the service provider to ensure system integrity. It does not include post-transmission storage of communications. For example, email that has been received by a recipient's service provider but has not yet been accessed by the recipient is in 'electronic storage.' *See Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 461 (5th Cir. 1994). At that stage, the communication is stored as a temporary and intermediate measure pending the recipient's retrieval of the communication from the service provider. Once the recipient retrieves the email, however, the communication reaches its final destination. If the recipient chooses to retain a copy of the accessed communication, the copy will not be in 'temporary, intermediate storage' and is not stored incident to transmission. *See Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2003) (stating that email in post-transmission storage was not in "temporary, intermediate storage"). By the same reasoning, if the sender of an email maintains a copy of the sent email, the copy will not be in 'electronic storage.' Messages posted to an electronic 'bulletin board' or similar service are also not in 'electronic storage' because the website on which they are posted is the final destination for the information. *See Snow v. DirecTV, Inc.*, 2005 WL 1226158, at *3 (M.D. Fla. May 9, 2005), *adopted by* 2005 WL 1266435 (M.D. Fla. May 27, 2005), *aff'd on other grounds*, 450 F.3d 1314 (11th Cir. 2006). http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf.

[25] *Theofel v. Farey Jones*, 359 F.3d 1066 (9th Cir. 2004).

[26] The Department of Justice Computer Crimes and Intellectual Property Section Manual describes the holding of the Ninth Circuit in *Theofel* as follows: "[T]he court held that email messages were in 'electronic storage' regardless of whether they had been previously accessed, because it concluded that retrieved email fell within the backup portion of the definition of 'electronic storage.' *Id.* at 1075-1077. Although the Ninth Circuit did not dispute that previously accessed email was not in temporary, intermediate storage within the meaning of § 2510(17)(A), it insisted that a previously accessed email message fell within the scope of the 'backup' portion of the definition of 'electronic storage,' because such a message "functions as a 'backup' for the user." *Id.* at 1075. The discomfort of some courts with the Justice Department's interpretation of the Stored Communications Act is evident in the Sixth Circuit's (now vacated) ruling in *Warshak v. United States* that "individuals maintain a reasonable expectation of privacy in emails that are stored with, or sent or received through, a commercial ISP." 532 F.3d 521, 536-537 (6th Cir. 2008). Specifically, the panel court upheld a preliminary injunction enjoining the government from "seizing the contents of a personal e-mail account" under 18 U.S.C. § 2703(d) unless the government provides prior notice to the e-mail user or shows that the e-mail user had no reasonable expectation of privacy vis-à-vis the e-mail service provider.

180 days old.[27] Likewise, while as a practical matter law enforcement must secure a warrant to access documents on a personal computer, under ECPA, a mere subpoena issued to a third party will suffice to access confidential documents stored remotely on the computers of a cloud computing service provider.[28]

The different standards are the unanticipated byproduct of technology changes, and not a careful balancing of the needs of law enforcement and the privacy rights of individuals. Nor do they reflect a substantive difference in the nature of the information; rather they reflect the fact that ECPA was enacted in 1986—six years before Congress authorized commercial activity on the Internet,[29] and seven years before the first web browser was introduced.[30] In 1986, very few Americans had e-mail accounts, and those who did typically downloaded email from a server onto their hard drives, and email was automatically and regularly overwritten by service providers grappling with storage constraints.[31] Even eight years later, when Congress enacted the Communications Assistance for Law Enforcement Act (CALEA),[32] the commercial Internet

---

27/ *See* DOJ, *Electronic Surveillance Manual*, at 25 (2005), *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf.

28/ 18 U.S.C. § 2703(b). While the government requires a warrant under Rule 41 to forcefully enter and seize someone's personal computer, it could theoretically choose to use a subpoena to compel production of the same computer or its contents, resorting to court enforcement if the recipient failed to comply with the subpoena. As a practical matter, however, concerns about compromising the investigation or destruction of evidence normally lead law enforcement to secure a warrant in this situation. The same concerns about compromise and loss of evidence are not normally present when the subpoena is served on a third party service or storage provider, however.

29/ Prior to 1992 the National Science Foundation's mandate was to support access to the Internet for research and education, and it had no authority to permit or promote commercial activity on the networks connecting research and academic institutions. This authority was conveyed to the NSF only in 1992, with passage of The Scientific and Advanced-Technology Act, 42 U.S.C. § 1862(g) (1992), which directed the National Science Foundation "to foster and support access by the research and education communities to computer networks which may be used substantially for purposes in addition to research and education in the sciences and engineering, if the additional uses will tend to increase the overall capabilities of the networks to support such research and education activities."

30/ The Mosaic web browser was released in 1993, a graphical browser developed by a team at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign (UIUC), led by Marc Andreessen.

31/ Achal Oza, *Amend the ECPA: Fourth Amendment Protection Erodes as E-Mails Get Dusty*, 88 B.U. L. Rev. 1043, 1072 (Note 2008) ("In 1986, e-mail technology was still very new. Most e-mail users dialed-up to their e-mail servers using a modem and downloaded their communications to a home computer, with the server acting only as a medium for temporary storage. Using this rationale, the ECPA draws a distinction between e-mails in electronic storage on third-party servers for 180 days or less and those in electronic storage longer than 180 days." Citing *Electronic Communications Privacy Act: Hearing on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. on the Judiciary*, 99th Cong. 475, at 24 (1986) (testimony of Philip M. Walker, General Regulatory Counsel, GTE Telenet Inc., and Vice Chairman, Electronic Mail Association)).

32/ Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001-1021).

was in its infancy, digital storage was expensive,[33] and email was automatically and regularly overwritten by service providers grappling with storage constraints.

Today, the distinctions between and among data in transit, data in electronic storage, data stored by a remote computing service, and data more them 180 days old no longer conform to the reasonable expectations of Americans, nor do these distinctions serve the public interest. A growing chorus of academics argues that these distinctions do not make sense,[34] and courts have had increasing difficulty applying ECPA. The Fifth Circuit described efforts to interpret the Wiretap Act as a "search for lightning bolts of comprehension [that] traverses a fog of inclusions and exclusions which obscures both the parties' burdens and the ultimate goal."[35] The Ninth Circuit described this as a "complex, often convoluted, area of the law."[36] In 2002 the Ninth Circuit said that Internet surveillance was "a confusing and uncertain area of the law" that is so out-dated that it is "ill-suited to address modern forms of communication."[37] A district court in Oregon recently opined that email is not covered by the Constitution, while the Ninth Circuit has

---

33/ Matt Komorowski, *A History of Storage Cost*, *available at* http://www.mkomo.com/cost-per-gigabyte (concludes that "space per unit cost has doubled roughly every 14 months," and states that "[s]everal terabyte+ drives have recently broken the $0.10/gigabyte barriers."); *see also* Digital Prosperity *supra* Note 5, at 8 (The falling cost of storage is "why Web companies like Google, Yahoo, and Microsoft are providing consumers with large amounts of free Web-based storage for their email, photos, and other files. For example, Google provides around 2.7 gigabytes (2,700 megabytes) of free storage for users of their Gmail e-mail service. If Google were to provide this service today using the technology of 1975 (in 2006 prices), it would cost them over $50 million per user! But because memory is now so cheap, Google and other companies can afford to give vast amounts of it away for free, paying for it through unobtrusive advertisements.").

34/ *See, e.g.*, Patricial L. Bellia, *Surveillance Law through Cyberlaw's Lens*, 72 Geo. Wash. L. Rev 1375, 1396-1397 (2004) (stating that "[s]tored communications have evolved in such a way that [ECPA's layer of statutory protection for stored communications], often referred to as the Stored Communications Act ("SCA"), are becoming increasingly outdated and difficult to apply."); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1234 (2004) (stating that the "strange" 180-day distinction "may reflect the Fourth Amendment abandonment doctrine at work," but concluding that "[i]ncorporating those weak Fourth Amendment principles into statutory law makes little sense").

35/ *Briggs v. Am. Air Filter Co.*, 630 F.2d 414, 415 (5th Cir. 1980) (Goldberg, J.). In a case involving the Wiretap Act and the Stored Communications Act, the same court said that the law is "famous (if not infamous) for its lack of clarity." *Steve Jackson Games, Inc. v. United States Secret Serv.*, 36 F.3d 457, 462 (5th Cir. 1994).

36/ *United States v. Smith*, 155 F.3d 1051, 1055 (9th Cir. 1998).

37/ *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002). The Ninth Circuit blamed this confusion on Congress's failure to update the law to take into account modern technologies. In particular, the court complained that: "the difficulty [in construing the surveillance statutes] is compounded by the fact that the ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication.... Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results." *Id.* While the Internet (but not the World Wide Web) did exist in 1986, it is entirely true that the Internet of 2010 bears very little resemblance to the Internet of 1986.

held that it is.[38/] Last year, a panel of the Sixth Circuit first ruled that email was protected by the Constitution and then a larger panel of the court vacated the opinion.[39/] The degree of uncertainty surrounding judicial application of ECPA requirements in any given situation makes it difficult for law enforcement and service providers alike to act with confidence. The absence of clear, intuitive rules necessarily complicates—and slows—business review of law enforcement requests. The absence of clear rules also makes businesses hesitant to embrace emerging Internet hosted services and complicates efforts to consolidate global data repositories.

As the Supreme Court has noted, clarity in the Fourth Amendment context benefits the public and law enforcement alike.[40/] Without clear rules, law enforcement personnel must either take the chance of stepping over the line-risking suppression of evidence or even personal sanctions - or shy away from the line to avoid overstepping.[41/] Neither law enforcement nor the public are well served when law enforcement cannot make appropriate use of an investigative tool because they do not know what is and is not allowed. A dramatic example of the negative consequences of the lack of clarity was cited by the Foreign Intelligence Surveillance Court of Review in *In Re Sealed Case*, where the court noted that the rules set forth in prior judicial decisions had been "very difficult... to administer."[42/] As the 9/11 Commission explained, in the days leading up to the 9/11 attacks, certain intelligence information was not shared with FBI agents who were familiar with al Qaeda because an intelligence analyst misunderstood those decisions and misapplied the Justice Department's rules implementing them.[43/] Lack of statutory

---

38/ *Compare In re United States,* 2009 WL 3416240 (D. Or. June 23, 2009), *with Quon v. Arch Wireless Operating Co.*, 529 F.3d. 892, 895-899 (9th Cir. 2008), *cert. granted* 130 S. Ct. 1101 (2009).

39/ *Warshak v. United States*, 490 F.3d 455, 467 (6th Cir.2007), *vacated en banc*, 532 F.3d 521 (6th Cir. 2008).

40/ *See, e.g., Arizona v. Roberson*, 486 U.S. 675, 681-682 (1988); *Oliver v. U.S.* , 466 U.S. 170, 181-182 (1984) ("This Court repeatedly has acknowledged the difficulties created for courts, police, and citizens by an ad hoc, case-by-case definition of Fourth Amendment standards to be applied in differing factual circumstances. The ad hoc approach not only makes it difficult for the policeman to discern the scope of his authority; it also creates a danger that constitutional rights will be arbitrarily and inequitably enforced." (citations omitted)).

41/ Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 Stan. L. Rev 503, 527-528 (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.... Clear rules announce ex ante what the police can and cannot do; so long as the police comply with the clear rules, the police will know that the evidence cannot be excluded.").

42/ *In re Sealed Case*, 310 F.3d 717, 743-744 (FISA Ct. Rev. 2002).

43/ *See id.* at 744; National Commission Terrorist Attacks Upon the United States, The 9/11 Commission Report at 78-80, 271, *available at* http://www.gpoaccess.gov/911/pdf/fullreport.pdf.

clarity also causes judicial uncertainty. When unclear statutory terms are interpreted differently in different federal jurisdictions, prosecutors are left with two choices: create different practices and procedures in each jurisdiction or adopt the most restrictive interpretation throughout the whole country. The first option can lead to confusion and arbitrary results, and the second can cause agents to forego the use of important investigative tools even where their use would be permissible.

As email has become a key means of personal and proprietary communications, and as users interact seamlessly with locally stored content and content stored on the Internet, ECPA's rules defy user expectation. Today, tens of millions of consumers enjoy free email and data storage services on the Internet.[44/] These services are normally advertising-supported, and service providers use automated tools to scan the communications in order to deliver relevant advertising or other services.[45/] Many service providers also examine content for security and anti-spam purposes.[46/] All of these activities are undertaken in connection with providing the communication service, and users do not expect that these activities somehow render their private communications less private. Indeed, the average webmail user would be surprised to learn that the government believes this to be the case. Applying ECPA to normal business practices in a manner that deprives users of basic privacy protections threatens to undermine information technology innovations such as cloud computing, which, "by altering the basic economics of access to computing and storage ... has the potential to reshape how U.S. and global businesses are organized and operate."[47/]

[44/] *See* Byron Acohido, *Microsoft takes notice as more people use free Google Docs*, USA Today, Sep. 22, 2009 (reporting that by July 2010 27% of companies plan to widely use Google Docs in the workplace).

[45/] *See* Google, More on Gmail and privacy, *available at* http://mail.google.com/mail/help/about_privacy.html#scanning_email

[46/] *See id.* ("Google scans the text of Gmail messages in order to filter spam and detect viruses, just as all major webmail services do.")

[47/] Jeffrey Rayport & Andrew Heyward, Andrew: *Envisioning the Cloud: the Next Computing Paradigm* (Mar. 20, 2009). According to the authors, cloud computing will lower capital requirements for technology start-ups, permit businesses to manage IT resources without tying up capital in IT capacity, while managing energy resources more efficiently; facilitate consumer access to an endless array of powerful applications at low cost; support innovation by reducing the human investment needed to build and maintain IT infrastructure; and foster cooperation and collaboration, without the coordination costs typically associated with bringing people and work together. *See* http://www.marketspaceadvisory.com/cloud/Envisioning-the-Cloud.pdf

As presently applied, ECPA does not comport with user expectations, does not meet law enforcement or judicial needs for clarity, creates non-trivial costs for businesses seeking to comply with law enforcement requests, and erects barriers to the adoption of innovative, productivity enhancing technology by American business. To address these deficiencies in a technology neutral manner, the consensus principles would bring all communications content, whether in transit or in storage (as commonly defined), notwithstanding the age of that content or the ordinary uses of that content by providers, under the basic probable cause standard set forth in the Fourth Amendment, accessible to law enforcement with a warrant.

Effect on Law Enforcement: This proposal would do no more than strictly necessary to reflect the reasonable expectations of privacy of communications technology users today, and to serve the public interest in facilitating innovation in the cloud. For example, the change:

- Would *not* extend to stored content the full range of protections that apply to real-time interception of communications content under the Wiretap Act, and would not require a "super warrant" for access to that data. Rather, this proposal does not modify the Wiretap Act,[48/] and under the proposal, a search warrant supported by probable cause would suffice to require a provider to disclose stored content;

- Would *not* further restrict the authority to access communications that are readily accessible to the general public, such as remarks posted on a blog or website available to the public;[49/]

- Would *not* modify the right of any authorized recipient of a communication, other than

---

48/ In 2000, the Justice Department supported legislation that would have extended the procedural protections accorded to voice interceptions to the real-time interception of electronic communications under the Wiretap Act, a change that the Justice Department supported in 2000. *See* Testimony of Kevin V. DiGregory, Deputy Assistant Attorney General, United States Department of Justice, Before the Subcommittee on the Constitution of the House Committee on the Judiciary on H.R. 5018 and H.R. 4987 (Sep. 6, 2000) ("For example, the Administration's package proposes that wiretaps for electronic communications should be treated just the same as voice wiretaps, including approval by a high-level Justice Department official, limited to the list of predicate crimes under §2516, and with the availability of suppression under §2515."), *available at* http://judiciary.house.gov/Legacy/digr0906.htm.

49/ 18 U.S.C. § 2511(2)(g)(1).

the service provider, to disclose data to the government without process. Thus, for example, anyone other than the service provider with authorized access to shared photos could voluntarily disclose those photos to anyone else, including a government agent;[50/]

- Would *not* change or eliminate any of the current exceptions permitting disclosures to the government by ECS and RCS providers, including those regarding inadvertently discovered evidence of a crime and emergency disclosures;

- *Would* establish uniform, clear, and easily understood rules about when and what kind of judicial review is needed by law enforcement to access electronic content; and

- *Would*, by clarifying the applicable rules, enable business to respond more quickly and with greater confidence to law enforcement requests and to avail themselves of hosted productivity technology.

Principle 2: Access to Mobile Location Data

Recommended Approach: Under the consensus principles, a governmental entity may require the provider of wire or electronic communications services to produce, prospectively or retrospectively, non-public information regarding the location of a mobile communications device only with a search warrant supported by probable cause.

Need for Change: Cell phones and mobile Internet devices generate location data to support both the underlying service and a growing range of location-based services of great convenience and value. A cell phone that is turned on—whether or not it is in use—is in near

---

[50/] One of the current exceptions—user consent—poses special issues, because, if broadly applied, consent would overwhelm all privacy protection. For government access, consent should not be inferred from, for example, Terms of Service that allow non-governmental entities to access content for various purposes. The recommendations are based on the presumption that the fact that a service provider has access to information in the cloud for purposes of providing the service, for offering value-added services or for delivering advertising does not diminish the user's expectation of privacy as against the government nor otherwise create any exception to the probable cause warrant requirement. This should be the case regardless of whether it is the provider or a third party contractor that is getting access for these business purposes. Rather, consent that would defeat the warrant requirement should have to be knowing, explicit, and specific both to the person who created the content and the content to be disclosed. If this is not clear, a further amendment may be appropriate.

constant communication with nearby cell towers,[51] and, as a result, site tower information always reveals something about a user's location (*i.e.*, what tower or towers are nearby). In urban areas, where there are many cell towers, a mobile communications device may communicate its location to more than one tower. By triangulating information received by two or more cell towers, it is possible to establish a user's location within a matter of yards.[52] This location data can be intercepted in real time and is often stored for research and development, resolution of billing disputes, and other business purposes;[53] it can reveal a very full picture of a person's movements, leading to inferences about activities and associations. In a growing number of devices, this automatically generated location data is augmented by very precise GPS data.[54]

The requirements governing access to location information are not clearly set out in ECPA. For years law enforcement treated cell site information as "signaling" or "addressing" information, obtained by simply certifying that the information—both retrospective and

---

[51] *See* DOJ, *Electronic Surveillance Manual*, at 40 (2005), *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf. ("A cell site simulator, digital analyzer, or a triggerfish can electronically force a cellular telephone to register its mobile identification number ('MIN,' *i.e.*, telephone number) and electronic serial number ('ESN,' *i.e.*, the number assigned by the manufacturer of the cellular telephone and programmed into the telephone) when the cellular telephone is turned on. Cell site data (the MIN, the ESN, and the channel and cell site codes identifying the cell location and geographical sub-sector from which the telephone is transmitting) are being transmitted continuously as a necessary aspect of cellular telephone call direction and processing. The necessary signaling data (ESN/MIN, channel/cell site codes) are not dialed or otherwise controlled by the cellular telephone user. Rather, the transmission of the cellular telephone's ESN/MIN to the nearest cell site occurs automatically when the cellular telephone is turned on. This automatic registration with the nearest cell site is the means by which the cellular service provider connects with and identifies the account, knows where to send calls, and reports constantly to the customer's telephone a read-out regarding the signal power, status and mode.")

[52] *See id.* at 41. The Global Positioning System (GPS), cell towers, and Wi-Fi positioning service (WPS) are the three techniques to identify a mobile device geo-location.

[53] *See* Declan McCullagh, *Feds Push for Tracking on Cell Phones*, Feb. 10, 2010, *available at* http://news.cnet.com/8301-13578_3-10451518-38.html ("Verizon Wireless keeps 'phone records including cell site location for 12 months,' [said] Drew Arena, Verizon's vice president and associate general counsel for law enforcement compliance.").

[54] The FCC's Enhanced 9-1-1 service will by 2012 require wireless carriers to have the ability to report information about a caller's location to within 50 to 300 meters when the caller makes an emergency call, and within 100 meters for most such calls. 47 C.F.R. § 20.18(h)(1); *see* FCC Enhanced 9-1-1—Wireless Services, *available at* http://www.fcc.gov/pshs/services/911-services/enhanced911/Welcome.html. Wireless carriers often meet this requirement by installing GPS capabilities in their devices. For example, all Verizon devices sold after 2003 are GPS-capable. *See* http://aboutus.vzw.com/wirelessissues/enhanced911.html.

prospective—was "relevant to an ongoing investigation."[55] In 1994 Congress amended the Pen Register statute to preclude the collection of information disclosing location "solely pursuant" to that statute.[56] Notwithstanding this change, until 2005 judges routinely issued orders based on the "relevant to an ongoing investigation" certification so long as the request identified any additional authority for the request.[57] Generally law enforcement cited the Stored Communications Act for this additional authority—even when the location information was sought on a prospective basis, on the theory that nothing in the Stored Communications Act "requires that the provider possess the records at the time the order is executed."[58]

In 2005, a magistrate judge in the Southern District of Texas rejected this so-called "hybrid-theory," holding – as most cell phone users would assume - that prospective collection of cell site data amounted to "tracking." Citing the standard for installing a mobile tracking device under 18 U.S.C. § 3117, the magistrate judge determined that law enforcement could access prospective cell site data only with a warrant supported by probable cause.[59] According

---

[55] *See* DOJ, *Electronic Surveillance Manual*, at 45 (2005), *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf. ("In 1994, the Office of Enforcement Operations opined that investigators did not need to obtain any legal process in order to use cell phone tracking devices so long as they did not capture the numbers dialed or other information 'traditionally' collected using a pen/trap device. This analysis concluded that the 'signaling information' automatically transmitted between a cell phone and the provider's tower does not implicate either the Fourth Amendment or the wiretap statute because it does not constitute the 'contents' of a communication. Moreover, the analysis reasoned—prior to the 2001 amendments—that the pen/trap statute did not apply to the collection of such information because of the narrow definitions of 'pen register' and 'trap and trace device.' Therefore, the guidance concluded, since neither the constitution nor any statute regulated their use, such devices did not require any legal authorization to operate.")

[56] Pub. L. 103-414, Title I, § 103 (1994) (codified at 47 U.S.C. § 1002(a)(2)). This preclusion is subject to an exception that applies to the extent the number itself provides the location, *i.e.*, for pay phones or wireline phones.

[57] *See* DOJ, *Electronic Surveillance Manual* at 41, 43-44, *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf. ("Because of the 1994 prohibition, law enforcement authorities have sought other means to compel providers to supply this information prospectively. Most commonly, investigators have used orders under section 2703(d) to obtain this information. Although section 2703(d) generally applies only to stored communications, nothing in that section requires that the provider possess the records at the time the order is executed. Moreover, use of such an order does not improperly evade the intent of the CALEA prohibition. Section 2703(d) court orders provide greater privacy protection and accountability than pen/trap orders by requiring (1) a greater factual showing by law enforcement and (2) an independent review of the facts by a court. Indeed, the very language of the CALEA prohibition—limiting its application 'to information acquired solely pursuant to the authority for pen registers and trap and trace devices'—indicates that Congress intended that the government be able to obtain this information using some other legal process. Public Law 103-414, sec. 103 (a) (emphasis supplied). Thus, 2703 (d) orders are an appropriate tool to compel a provider to collect cell phone location information prospectively." According to the DOJ Manual "[l]aw enforcement investigators may use … an order under section 2703(d) of title 18 in order to obtain historical records from cellular carriers.")

[58] *Id.*

[59] *In Re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority United States District Court*, Southern District of Texas, Houston Division, Magistrate No. H-05-557M (Oct. 14, 2005).

to Judge Smith, "While the cell phone was not originally conceived as a tracking device, law enforcement converts it to that purpose by monitoring cell site data." Magistrate judges around the country followed Judge Smith's lead on this, including a majority of the opinions published since 2005.[60]

Although Judge Smith's opinion applied only to the *prospective* collection of cell-site information, he noted that an individual might have "an objectively reasonable privacy interest in caller location information,"[61] based on the Fourth Amendment as well as the Wireless Communication and Public Safety Act of 1999.[62] He rejected the notion that there is no reasonable expectation of privacy in cell site location data, as well as the government's attempt to analogize cell site data to telephone numbers found unprotected in *Smith v. Maryland,* 442 U.S. 735 (1979): "Unlike dialed telephone numbers, cell site data is not "voluntarily conveyed" by the user to the phone company. As we have seen, it is transmitted automatically during the registration process, entirely independent of the user's input, control, or knowledge … location information is a special class of customer information, which can only be used or disclosed in an emergency situation, absent express prior consent by the customer."[63]

More recently, courts have rejected government requests for retrospective location data without a warrant, citing the language of the Stored Communications Act that "expressly sets movement/location information outside its scope by defining "electronic communications" to exclude "any communication from a tracking device" (as defined in 18 U.S.C. § 3117) and noting that the "electronic communications statutes, correctly interpreted, do not distinguish

---

60/ *See* Declan McCullagh, *Feds Push for Tracking on Cell Phones*, Feb. 10, 2010, *available at* http://news.cnet.com/8301-13578_3-10451518-38.html ("Only a minority [of judges] has sided with the Justice Department [on rules regarding prospective cell phone tracking]."); Transcript of Town Hall Record, *Beyond Voice: Mapping the Mobile Marketplace*, at 177-178 (May 6, 2008) (Session 4, "Location-Based Services"), *available at* http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/050608_sess4.pdf.

61 *In Re Application for Pen Register*, supra note 58 at 16.

62/ Pub. L. No. 106-81, § 5, 113 Stat. 1288 (Oct. 26, 1999) (codified at 47 U.S.C. § 222(f)).

63/ *In Re Application for Pen Register*, supra note 58 at 15; http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf.

between historic and prospective [cell site location information]."[64] Under these holdings, law enforcement can no longer assume that they will be able to acquire location data without a warrant based on probable cause.

Courts that require law enforcement to secure a warrant based on probable cause to access mobile location data recognize that users are likely to assume that tracking, however accomplished, is still tracking. To comport with reasonable expectations and serve the public interest, the current uncertainty should be resolved by applying the probable cause standard to disclosure of relatively precise location information.

There are already a number of innovative, socially beneficial "location aware" applications that employ technologies such as GPS, cell phone infrastructure, or wireless access points to locate electronic devices and provide "resources such as a 'you are here' marker on a city map, reviews for restaurants in the area, a nap alarm triggered by your specific stop on a commuter train, or notices about nearby bottlenecks in traffic."[65] More applications such as these are emerging every day, and in short order "systems which create and store digital records of people's movements through public space will be woven inextricably into the fabric of everyday life."[66] These applications will enhance quality of life, further important economic and social goals, and—with appropriate safeguards—serve law enforcement. Absent clear standards, privacy concerns could discourage consumer use, which could in turn make it less likely that location data will be available to law enforcement with proper authority.

---

[64] *In the Matter of the Application of the United States of America for an Order Directing the Provider of Electronic Communications Service to Disclose Records to the Government*, U.S. District Court for the Western District of Pennsylvania. Magistrate's No. 07-524M Magistrate Judge Lisa Pupo Lenihan , *aff'd* Sep. 2008, ("Government's requests for Court Orders mandating a cell phone service provider's covert disclosure of individual subscribers' (and possibly others') physical location information must be accompanied by a showing of probable cause."). The case has been appealed to the Third Circuit, which heard oral arguments on February 12, 2010. Case 08-4227.

[65] *See* Educause Learning Initiative, *7 Things You Should Know About ... Location Aware Applications*, *available at* http://net.educause.edu/ir/library/pdf/ELI7047.pdf.

[66] Andrew J. Blumberg & Peter Eckersley, Electronic Frontier Foundation, *On Locational Privacy, and How to Avoid Losing it Forever*, at 1 (Aug. 2009), *available at* http://www.eff.org/files/eff-locational-privacy.pdf. The sensitivity of precise geographic location information was also discussed at a panel on mobile "location-based services" during the FTC's 2008 Town Hall on mobile marketing. *See* Transcript of Town Hall Record, *Beyond Voice: Mapping the Mobile Marketplace* (May 6, 2008) (Session 4, "Location-Based Services"), *available at* http://htc-01.media.globix.net/COMP008760MOD1/ftc_web/transcripts/050608_sess4.pdf.

Effect on Law Enforcement: Information that reveals an individual's precise location can be highly sensitive, and collection of this information without proper safeguards implicates the exercise of a variety of rights protected by the Constitution, including important expression and association rights. To facilitate innovation, encourage the uptake of emerging location-aware technologies, and ensure that law enforcement access to location information generated by these products and services comports with the reasonable privacy expectations of Americans, ECPA should be amended to require a warrant based on probable cause to support access to location information, whether it is sought on a retrospective or prospective basis.[67] This standard is consistent with Fourth Amendment safeguards against unreasonable search and seizure. In many cases, law enforcement must already meet the probable cause standard when requesting location data,[68] and certain service providers are taking the position that location data is subject to higher standards under ECPA for content.[69]

Principle 3: Access to Transactional Data

Recommended Approach: Under the consensus principles, a governmental entity could require the provider of wire or electronic communications services to produce, prospectively or in real time, transactional information (*i.e.*, dialed number information, IP address, Internet port information, email to/from information and similar communications traffic data)[70] only with a judicial finding that the entity has offered specific and articulable facts demonstrating reasonable

---

[67] This would be subject, of course, to the exception for telephone numbers that themselves provide location information.

[68] Most courts have held that prospective information requires a showing of probable cause. See *supra* note 63. Law enforcement requests for retrospective location data are often combined with requests for prospective data. *See, e.g., In re Application Of The United States Of America For An Order Directing A Provider Of Electronic Communication Service To Disclose Records To The Government*, 534 F. Supp. 2d 585, 589 (W.D. Pa. 2008); *In re Application of U.S. for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone*, 460 F. Supp. 2d 448, 453 (S.D.N.Y. 2006).

[69] For example, the Loopt service "shows users where friends are located and what they are doing via detailed, interactive maps on their mobile phones.... Users can also share location updates, geo-tagged photos and comments with friends in their mobile address book or on online social networks, communities and blogs." The provider clearly understands the privacy implications of this technology, and reassures users that "Loopt was designed with user privacy at its core and offers a variety of effective and intuitive privacy controls." About Loopt, *available at* http://www.loopt.com/about.

[70] DOJ, *Electronic Surveillance Manual,* at 39 (2005), *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf. ("Pen register and trap and trace devices may obtain any noncontent information—all 'dialing, routing, addressing, and signaling information'—utilized in the processing and transmitting of wire and electronic communications. Such information includes IP addresses and port numbers, as well as the 'To' and 'From' information contained in an e-mail header.")

grounds to believe the information sought is relevant and material to an ongoing criminal investigation.

Need for Change: Transactional data—records of who is calling whom, when and for how long, and records of all the "to" and "from" information associated with one's email, including date, time, message length (including subject line length)—can be highly revealing. Transactional records for e-mail and cell phone usage may contain far more information about an individual's communications than "pen register" data in the wireline environment of the 1980s.[71] As technology has evolved, transactional data has become ever more detailed and revealing, but remains available to law enforcement without effective judicial supervision. In fact, under ECPA, a court *must* issue an order for a pen register[72] or trap and trace device[73] whenever a prosecutor files a document stating that the information sought is relevant to an ongoing investigation.[74] Thus, read literally, a judge cannot even assess whether the information is in fact relevant; the only question is whether the government says that it is. As communications technology evolves and produces increasingly detailed and rich transactional

---

[71] For example, the transactional record of an outgoing phone call to someone in a large office likely only contains the general office phone number and does not specify which person in the office has been contacted. However, the transactional record of an email to that person contains the recipient's unique email address. *See* Center for Democracy & Technology's Analysis of S.2092 (Apr. 4, 2000), *available at* http://old.cdt.org/security/000404amending.shtml.

It is not yet clear whether information such as URL's that include search terms or specific website addresses are "content" information that must be excluded from transactional records. Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 Wm. & Mary L. Rev 2105, 2105 (2009) ("Courts and Internet law scholars have yet to offer a means of determining the content/envelope status of unique aspects of Internet communications-from email subject lines to website URLs."). If transactional records for e-mail or Internet-enabled cell phones include this information, then they would be far more revealing than traditional wireline telephone records. *E.g.*, *United States v. Forrester*, 512 F.3d 500, 510 n.6 (9th Cir. 2008) ("Surveillance techniques that enable the government to determine not only the IP addresses that a person accesses but also the uniform resource locators ("URL") of the pages visited might be more constitutionally problematic. A URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person's Internet activity.").

[72] A "pen register" is defined as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication...." 18 U.S.C. § 3127(3).

[73] A "trap and trace device" is defined as a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, [or] signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however that such information shall not include the contents of any communication. 18 U.S.C. § 3127(4).

[74] 18 U.S.C. § 3123(a).

information, it is appropriate to afford judges a meaningful role in assessing whether the government's claim of relevance is substantiated.

Effect on Law Enforcement: The Justice Department has in the past acknowledged that the approach taken by the recommended principle is appropriate.[75] Nonetheless, the consensus principles call for a modest change only: The standard proposed is significantly less than probable cause: "specific and articulable facts showing that there are reasonable grounds to believe that the information … is relevant and material." Drawn from the *Terry* decision of the U.S. Supreme Court,[76] the language is identical to the formulation in the Stored Communications Act, which currently provides:

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.[77]

The marginal burden on law enforcement from this change should be minimal because law enforcement rarely asks for a pen register order without already possessing information sufficient to satisfy a "specific and articulable facts" standard.[78] The change will enhance business

---

[75] *See* DOJ's View on H.R. 5018 (Electronic Communications Privacy Act of 2000), Testimony of Kevin Digregory, Deputy Associate Attorney General, *available at* http://commdocs.house.gov/committees/judiciary/hju67343.000/hju67343_0.htm ("H.R. 5018, like the Administration's bill, would introduce the requirement of judicial review of the factual basis for such orders. Specifically, H.R. 5018 would require such applications to contain 'specific and articulable facts' that would justify the collection of the data. While the Justice Department can comply with the added administrative burdens imposed by increasing this standard, we have concerns about the amendments. Specifically, the technology-specific manner in which the bill would implement this change, the lack of an emergency exception, and the unrealistic geographic limitations that restrict such orders in the present law all raise serious concerns that should be addressed.").

[76] *Terry v. Ohio*, 392 U.S. 1, 21 (1968).

[77] 18 U.S.C. § 2703(d).

[78] Orin S. Kerr, *Internet Surveillance Law after the USA Patriot Act: The Big Brother That Isn't*, 97 Nw. U. L. Rev. 607, 639 & 673 n. 154 (2003) ("[A] higher 'specific and articulable facts' threshold would not add substantial burden for law enforcement…. [I]n my government experience I never knew or even heard of any law enforcement agent or lawyer obtaining a pen register order when the agent did not also have specific and articulable facts, which would satisfy the higher threshold. My experience is narrow, but it suggests that the practical burden of obtaining the order combined with the certification to a federal judge and potential for criminal liability effectively regulates government officers and deters them from obtaining pen register orders in bad faith. On the other hand, there may be rogue officers out there, if not now then in the future, and a higher threshold combined with judicial review could potentially provide an extra barrier to abuse.").

responsiveness by clarifying the obligations of both law enforcement and business, and preserves the distinction between content and transactional data, and maintains the reduced burden needed to acquire the latter.

Principle 4: Access to Subscriber Identifying Data and Stored Transactional Information

Recommended Approach: Under the consensus principles, a governmental entity may use a subpoena to require the provider of wire or electronic communications services to produce information related to a specified account or individual. Judicial approval would be necessary only where such requests do not relate to a specified account or individual.

Need for Change: Under ECPA, law enforcement may use an administrative, grand jury or trial subpoena to acquire certain information pertaining to a "subscriber to or [a] customer" of an electronic communications service or remote computing service.[79/] The information that may be acquired under this provision includes name, address, call or session records, length of service and type of service utilized, and method of payment.[80/] Using the administrative subpoena authority, law enforcement makes an independent determination that certain records are needed and then issues and serves the subpoena without input from a grand jury or even an assistant U.S. Attorney. Such administrative subpoenas are subject to judicial review only if the recipient of the subpoena challenges it. With administrative, grand jury or trial subpoenas, the government has no obligation to notify the subscriber or customer to whom the records relate.[81/] A carrier or ISP will rarely have the incentive to challenge a subpoena, so this information is routinely disclosed without any judicial review whatsoever.

The absence of judicial review or any meaningful opportunity to challenge a request for subscriber identifying records and stored customer records suggests that the scope of the subpoenas in these cases should be appropriately tailored. Indeed, the language of the statute itself suggests that such subpoenas may be issued for information pertaining to "a subscriber" or "a customer" identified with some particularity, for example, by a phone number or an IP

79/ 18 U.S.C. § 2703(c)(2).

80/ *Id.*

81/ 18 U.S.C. § 2703(c)(3).

address at a specific time. This principle would make it clear that a subpoena cannot be used to compel production of, for example, information identifying "*all* subscribers" whose device registered on a specified cell tower on a specified date, or information identifying "*all* subscribers" who accessed a particular web site during a specified period of time. Nothing in the legislative history of ECPA suggests that the provision should be read to authorize such broad use of subpoenas. Rather, the absence of judicial review argues for a narrow interpretation to avoid misuse of the subpoena for "fishing expeditions."[82/]

Effect on Law Enforcement: The principle is intended to clarify that the government may use a subpoena to obtain the subscriber information specified in the statute if the investigator can identify the subscriber with particularity (*e.g.* phone number, IP address used at a specific time). Otherwise, the investigator would obtain the information after securing a §2703(d) order based on specific and articulable facts demonstrating reasonable grounds to believe that the information is relevant to an ongoing criminal investigation, or a search warrant. The consensus principles would leave the current standard found in ECPA untouched when the records sought by law enforcement pertain to a specific subscriber or customer. Only if the government sought records about groups of subscribers or customers, would judicial review be required.

Conclusion

The United States leads the world in bringing innovative, ground-breaking communications technology to market, and enjoys the many social and economic benefits that technology produces. The United States also enjoys the many benefits flowing from Constitutional safeguards designed to preserve individual liberties, including the right to be free from unreasonable search and seizure. The U.S. has consistently balanced those values with the

---

82/ Without a narrow interpretation, law enforcement can subpoena a list of all visitors to a news website on a particular day, and order that the recipient of the subpoena not disclose the subpoena's existence. The Department of Justice recently attempted this before withdrawing its subpoena after the website owners objected publicly. *See* Declan McCullagh, *Justice Dept. Asked for News Site's Visitor Lists*, Taking Liberties Blog (Nov. 10, 2009), *available at* http://www.cbsnews.com/blogs/2009/11/09/taking_liberties/entry5595506.shtml; Copy of Subpoena, *available at* http://www.eff.org/files/subpoena.pdf. *See also* Nymity Interview, *Where Did Due Process Go? Government Access to Personal Information in the Cloud* (Interview with Scott Shipman, eBay) (Feb 2010), http://www.nymity.com/Free_Privacy_Resources/Privacy_Interviews/2010/Scott_Shipman.aspx ("[W]e're starting to see a new wave of requests. These new requests are a broad request for a large group of unnamed customers. For example, we see requests from authorities that state, 'please provide all information on all sellers who have sold in the following jurisdiction (zip code) within the last year.' Requests like those arguably flip the notion of due process upside down.").

needs of law enforcement in the communications environment, and both U.S. consumers and the U.S. economy have benefitted from the trust and confidence that this balance inspires in our electronic communications and information technology services providers, including among businesses and individuals located outside our borders. Changes in technology since 1986 have made it difficult to apply ECPA in a manner that comports with the reasonable expectations of individuals, potentially eroding user willingness to entrust private information to third party service providers in the United States. The principles recommended by the working group would, if implemented, align ECPA with current and emerging technology without unduly constraining or imposing significant burdens on law enforcement.

6.805
Fourth Amendment

10/11

Prelim Oct 4 Page Sore memo on NN due today
- nan late
- I was not aware of

---

2 weeks on 4th amendment
+ electronic survalance law
big data

Semayne - ~~Palace~~ a man's home is his castle
privacy
1604

Things the king (gaernment) can do
When can ga enter their house
1. Process
- warrent
- document approved by court

(2)

English common law - name of document

if leave door open - no can just walk in
not the case today

(missed some)

2. Reason / Cause
from detached / neutral magistrate

3. Must ask as well
"knock and announce"
Civility

This is pretty much the rule

Today police must leave a copy of the warrant
Only for the property owner
lots of exceptions
- hot pursuit

(3)

Cars not really that protected

---

don't need to give notice on electronic surveillance

troubled law makers + legal ~~scan~~ scolds

might never know

Secret search

founders were worried about unlim power of state

Congress added 2 provisions

"Super warrant"

must show have tried other mechanisms

~~Title~~ Evolving use of Tech

1928 only telephone

Crime

prohibition

large scale conspiracy

Taft was MoC, Chief Justice, President

Secretary of War

(9)

Other cases he cites

Boyd - law compelled production of documents
but if no docs → confession

5th amend - right not to self incriminate

But this was voluntary

Person, papers, effects

Phone convo is not those!

Olmstead argues its more than that

Boyd argues its more than that
└ never seized papers in Boyd

Argument: case shows Court is willing to expand defn

Justice: Boyd is really a 5th amnd case
just catered to papers

(5)

So 4A model: property

tapping off property → so no trespass
not the wires of Olmstead
no actual trespass
like Semayne
"bright line rule"

laws are written w/ the evils that already happened

Brandeis: permissive, expansionist view
not talismanic rules
↑ exactly as mentioned

looks at same cases and interprets them the complete other way!

held in trust by gov - so extended your property interest in it - mail
reasonable expectation of privacy

(6)

What are your expectations?

- on mail
- on telephone

expectations doctrine - fairly liberal / expansionist

What was Brandises' main concern?

Government violates our rule for more evidence

Make a future argument - what if tech was much further at

- slight of hand?
- very reasonable?
- overreaching?

Other privacy related - Justice Brandise?

HLS: Right to Privacy article
- 1900s

Brandise lost

(1)

Katz:

1968

Phone booth

Shuts door

gambled

public phone booth

telephones widespread now

Org crime tie in:

└ was big social threat:

Closed door → expectation of privacy:

protected interest intruded upon:

- How does he court get there:

Can make 2 arguments at once

8

Do Not Call case relied on sanctity of home
Did it turn away from katz?

~1968 Congress passed rules allowing wire tapping

When is an expectation reasonable?

(missed)
Up to courts to ascertain
Looking for broad purpose for 4th amendment

expectations were subjective

Said to legislature + please clarify

What protections society should have from gov intrusion

1986 Congress Electronic Communications Privacy Act
preemptive strike

(9)

Electronic Mail + Remote Computing Services

more like 1st class letter or telegraph
(did need warrant) (never req a warrant)
store + forward
b/w private individuals
stored at multiple pts along the way

---

expectation of privacy in email?
not many users
email Cos tried to make preemptive strike

---

plus well known Corp. espionage

Since email handled by 17 third parties

why does it depend if email downloaded from server?
Or that it was read

~~Prof: you left it lying around~~

These were "objective" decisions Congress made

(10)

Alan: We would have been better off w/o it

Congress had mainframe mental model

Could argue in 86 - protections not there

But today, Courts would argue more protection than ECPA gave it

Spirit of ECPA to provide more protections

But not written at all for webmail

Also 180 day distinction

Warrant vs Subpoena

↑ judge
harder
probable cause for crime

↑ grand jury
prosecutor
easy esp for domestic
relevant to ongoing investigation

(11)

1994 transactional records
2703(d)

2703(d) → half way b/w warrant & subpoena
Specific + articulable facts

Terry
limited touching
between stopping on street and arrest
need probable cause to talk to someone

What don't really want → police stopping everyone
Subpoena is pretty much a general search

Email gray area
logs
temp copies

(12)

URLs/ Headers were kinda messages

- didn't want warrant - too hard
- didn't want subpoena - too loose

So intermediate Terry standard

For transactional records

Diff standards make a big difference

above wiretapping

Level 3 wiretapping

Warrant w/ probable cause

minimization

particularity

inventory

notification

90 day renewal

"super warrant"

13

Many procedural standards don't exist here
So in real world yet broad access

Subpoenas can be challenged
Often time co gets one
Some cos realize biz interest in ~~bad~~ fighting subpoenas
Also: At Google they got one for their entire index
Only one that went to court
Which is risky since FBI + Justice dept
Operate on good guy/bad guy distinction

Info companies are last line of deciding if order is valid

2001 Patriot Act
terrorism
national security letter
thought very severe threat

(14)

Warrant crime were one very seperate

How many intrusions are allowed?

So 4th Ammendment is very complicated

- location
- 180 day rule
- gov looking at large amts of data
  - prediction

Break

Group Projects

Steven absent

Next week: clear issue statement

Specific policy rec

Who mentor

(15)

Next week
how divide work
Schedule meeting w/ mentor

Staff vs outside mentor vs Comm mentors
1 teacher adapted each group

Privacy
guidelines for whom?
be able answer for next week.

Circumvention
TOR
Scope under

Mobile Data Privacy
narrow (everyone doing that!)
Gov access for 3rd party

(6)

Elasticity of law w/ new tech

Content vs media headers

Cloud service vs desktop vs in flight

What policies to be consistent

---

if do legal issue - read LexisNexis Academic Universe
lots of law students

Copyright A

SOPA + PIPA

major issues w/ SOPA

recommend changes

international

Central db

Prof: both indv sections + overall approach

(17)

What kinda approach are you proposing?
SOPA 2 as controversial as SOPA 1

- Tech approach
- Legislation written

Prof: Need Strategy not legislation drafting
Wiel - from RIAA

Copyright B

Policy rec for Dept of Ed
Open Textbooks
(they went totally diff)
incentive writing + use
Digital lib
Scan books
Open standards
tech or policy?

(18)

Curriculm shared online

HW

Subsidy

Kindle

iPad

More on policy - then build a product

Copyright

Cybersecurity

workable national policy for offensive

White House

ethical, legal concerns

what authorized to do?

statements?

reward sanctions

(19)

UAVs

private sector use

support legit use + discourage abuse

federal or state issue?

Camera law

FAA - where can fly

privacy law about house

Internet Governance

NTIA

currently US hosts a lot of these

Foreign govs want control

foreign policy

+ domestic issue

technical issue

Prof's pick | institution

(20)

3rd Party Data Collection

Best practices
think about how policy rec

Vs

1 or 2
need mentors
or totally diff
Speeding tickets
framework for analysis ← is key

Part 1: Framework
2: 1-2-3 to eval
can do more

Should do minor changes to proposal

Revise Proposal

10/11

Graduated Response
Copyright Lawsuits - logical pair

Write that up in a paragraph

Analyze Stephen's writing ...

10/13

6.805 Semester Project Proposal

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

2012 saw the reemergence of copyright legislation in the public consciousness, especially in the wake of SOPA and PIPA, which sought to combat piracy on the Internet. The resulting backlash against these bills—both from Internet users and businesses themselves, as well as from political opposition—indicate divisive attitudes over the effectiveness of the proposed anti-piracy mechanisms. Our project aims to develop a framework for the cost-benefit analysis of such anti-piracy mechanisms. In order to do this, we will design a model that will evaluate different metrics of effectiveness and pose a number of questions. Will the policy actually make a difference? Can the policy be implemented robustly? Can pirates easily avoid the mechanism? What are the costs and challenges of implementation? Does the policy violate the standards of the Internet? Will the policy prevent us from accomplishing other goals, such as tightening up cyber security? Will certain actors incur a cost, and if so, who will pay for it? To supplement this analysis, we will review existing literature on the economic costs of online piracy and develop a system of classifying these losses.

not good lang (my section)

Based on these issues, the long-term goal for this evaluative framework will be to encompass a common set of values, standards, and metrics for the analysis and discussion of future proposed anti-piracy mechanisms. With this model, we hope to enable a more robust discussion of how to address the piracy problem without compromising the underlying structures of the open Internet and—by extension—the civil liberties guaranteed by those structures and the ecosystem for innovation that they have enabled. This analysis will also take into account pragmatic issues of economic costs, possible political challenges, and other barriers to comprehensive implementation. We will also be sure to examine copyright law pre- and post- Internet, to see how notions of intellectual property and proper enforcement of those exclusive rights have changed over time, in order to better contextualize the issue.

✓

To illustrate the usefulness of such a framework, we will show it in action by running a analysis of recent graduated response policies proposed to combat online piracy—specifically, the HADOPI law in France and the "six strikes" Copyright Alert System being implemented here in the US as part of an agreement between the MPAA, the RIAA, and a number of major ISPs. To put this assessment into perspective, we will also use our framework to evaluate the effectiveness of the previous anti-piracy paradigm of filing lawsuits against individual users, using it as a benchmark for comparison. Through this analysis, we will be able to identify the merits and downsides of graduated response mechanisms, discuss them in relation to traditional copyright litigation strategies, and provide comprehensive policy suggestions. Ideally, the framework we develop in this project can also be extended to other anti-piracy mechanisms and create a more standardized system for analyzing and deciding between these kinds of policies.

nice

Individual writing assignment for next week: Memo on Net Neutrality

Due October 10 on Stellar Opps - just heard about on Thurs

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

- makes previous judgement void

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

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

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

NN all together or case?

Bullet Pts :)

10/13
Late

Net Neutrality Memo

Michael Plasmeier[1]

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

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

Proponents

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

Opponents

Big ISPs: AT&T, Comcast, Verizon

Arguments for net neutrality

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

Arguments against net neutrality:

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

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

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

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

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

Recent Court Case

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

Moving Forward

Reclassification

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

Congress's Role

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

Talking Points

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

Class 7, Oct 18, 2012 - Fourth Amendment: Big and Linked Data

Class 7, Oct 18: 2012 - Fourth Amendment: Big Data and Linked Data

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

Goals

This week's class explores the challenges to Fourth Amendment jurisprudence from the need to adapt to new technologies that extend governments' capabilities to perform remote sensing and data collection.

Class Preparation

There are a lot of cases here, but please read them carefully, because they are critical to today's debates over privacy and government surveillance. We suggest briefing the cases as you study. (There's no need to hand in the briefs.)

Privacy interest in information held by 'third parties'

- *Smith v. Maryland*, 442 U.S 735 (1979). Landmark Supreme court ruling on Fourth Amendment status of telephone records
- *U.S. v. Maynard*, DC Cir 08-3030 (August 2010). Read the whole opinion, but focus on the case of Jones. Can federal agents install a GPS unit on your car, without a warrant? What is the difference between the "whole" and the "sum of the parts"?
- *U.S. v. Miller*, 425 U.S. 435 (1976). Do you have a legal right to privacy of your bank records?

Adapting to new sensing technologies

- Kyllo v. United States (99-8508) 533 U.S. 27 (2001). Is a "search" a seach when there is no physical intrusion?
- US v. Jones (2012) Does GPS tracking over a long period of time require a probable cause warrant?

Government power in 'special circumstances' - terrorism and threats to national security

- City of Indianapolis et al. v. Edmon et al. 531 U.S. 32 (2000). Can law enforcement set up roadblocks for conducting random drug searches?

The inference and analytics

- New York Times: Jeff Rosen, Total Information Awareness, Dec 15, 2002
- Office of the Director of National Intelligence release on new Attorney General "Guidelines for Access, Retention, Use, and Dissemination by the National Counterrorism Center (NCTC) of Information in Datasets Containing Non-Terrorism Information" (read the release and skim the guidelines.)
- New York Times: U.S. Relaxes Limits on Use of Data in Terror Analysis (March 22, 2012)
- EFF analysis of the guidelines

Agenda 2013 Activity

Three-minute oral team reports, similar to last week, but wth more about your specific approach, interaction with mentors, and tighter topics and conclusions.

Assignment for next week (Oct. 25)

To be announced: Watch this space.

U.S. Supreme Court

SMITH v. MARYLAND, 442 U.S. 735 (1979)

442 U.S. 735

SMITH v. MARYLAND.
CERTIORARI TO THE COURT OF APPEALS OF MARYLAND.

No. 78-5374.

Argued March 28, 1979.
Decided June 20, 1979.

The telephone company, at police request, installed at its central offices a pen register to record the numbers dialed from the telephone at petitioner's home. Prior to his robbery trial, petitioner moved to suppress "all fruits derived from" the pen register. The Maryland trial court denied this motion, holding that the warrantless installation of the pen register did not violate the Fourth Amendment. Petitioner was convicted, and the Maryland Court of Appeals affirmed.

Pen register ≠ search

Held:

The installation and use of the pen register was not a "search" within the meaning of the Fourth Amendment, and hence no warrant was required. Pp. 739-746.

(a) Application of the Fourth Amendment depends on whether the person invoking its protection can claim a "legitimate expectation of privacy" that has been invaded by government action. This inquiry normally embraces two questions: first, whether the individual has exhibited an actual (subjective) expectation of privacy; and second, whether his expectation is one that society is prepared to recognize as "reasonable." Katz v. United States, 389 U.S. 347 . Pp. 739-741.

(b) Petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and even if he did, his expectation was not "legitimate." First, it is doubtful that telephone users in general have any expectation of privacy regarding the numbers they dial, since they typically know that they must convey phone numbers to the telephone company and that the company has facilities for recording this information and does in fact record it for various legitimate business purposes. And petitioner did not demonstrate an expectation of privacy merely by using his home phone rather than some other phone, since his conduct, although perhaps calculated to keep the contents of his conversation private, was not calculated to preserve the privacy of the number he dialed. Second, even if petitioner did harbor some subjective expectation of privacy, this expectation was not one that society is prepared to recognize as "reasonable." When petitioner voluntarily conveyed numerical information to the phone company and "exposed" that information to its equipment in the normal course of business, he assumed the risk that the company would reveal the information [442 U.S. 735, 736] to

So URLs?

the police, cf. United States v. Miller, 425 U.S. 435 . Pp. 741-746.

283 Md. 156, 389 A. 2d 858, affirmed.

BLACKMUN, J., delivered the opinion of the Court, in which BURGER, C. J., and WHITE, REHNQUIST, and STEVENS, JJ., joined. STEWART, J., post, p. 746, and MARSHALL, J., post, p. 748, filed dissenting opinions, in which BRENNAN, J., joined. POWELL, J., took no part in the consideration or decision of the case.

Howard L. Cardin argued the cause for petitioner. With him on the brief was James J. Gitomer.

Stephen H. Sachs, Attorney General of Maryland, argued the cause for respondent. With him on the brief were George A. Nilson, Deputy Attorney General, and Deborah K. Handel and Stephen B. Caplis, Assistant Attorneys General.

MR. JUSTICE BLACKMUN delivered the opinion of the Court.

This case presents the question whether the installation and use of a pen register 1 constitutes a "search" within the meaning of the Fourth Amendment, 2 made applicable to the States through the Fourteenth Amendment. Mapp v. Ohio, 367 U.S. 643 (1961). [442 U.S. 735, 737]

I

On March 5, 1976, in Baltimore, Md., Patricia McDonough was robbed. She gave the police a description of the robber and of a 1975 Monte Carlo automobile she had observed near the scene of the crime. Tr. 66-68. After the robbery, McDonough began receiving threatening and obscene phone calls from a man identifying himself as the robber. On one occasion, the caller asked that she step out on her front porch; she did so, and saw the 1975 Monte Carlo she had earlier described to police moving slowly past her home. Id., at 70. On March 16, police spotted a man who met McDonough's description driving a 1975 Monte Carlo in her neighborhood. Id., at 71-72. By tracing the license plate number, police learned that the car was registered in the name of petitioner, Michael Lee Smith. Id., at 72.

The next day, the telephone company, at police request, installed a pen register at its central offices to record the numbers dialed from the telephone at petitioner's home. Id., at 73, 75. The police did not get a warrant or court order before having the pen register installed. The register revealed that on March 17 a call was placed from petitioner's home to McDonough's phone. Id., at 74. On the basis of this and other evidence, the police obtained a warrant to search petitioner's residence. Id., at 75. The search revealed that a page in petitioner's phone book was turned down to the name and number of Patricia McDonough; the phone book was seized. Ibid. Petitioner was arrested, and a six-man lineup was held on March 19. McDonough identified petitioner as the man who had robbed her. Id., at 70-71.

Petitioner was indicted in the Criminal Court of Baltimore for robbery. By pretrial motion, he sought to suppress "all fruits derived from the pen register" on the ground that the police had failed to secure a warrant prior to its installation. Record 14; Tr. 54-56. The trial court denied the suppression motion, holding that the warrantless installation of the pen [442 U.S. 735, 738] register did not violate the Fourth Amendment. Id., at 63. Petitioner then waived a jury, and the case was submitted to the court on an agreed statement of facts. Id., at 65-66. The pen register tape (evidencing the fact that a phone call had been made from petitioner's phone to McDonough's phone) and the phone book seized in the search of petitioner's residence were admitted into evidence against him. Id., at 74-76. Petitioner was convicted, id., at 78, and was sentenced to six years. He appealed to the Maryland Court of Special Appeals, but

the Court of Appeals of Maryland issued a writ of certiorari to the intermediate court in advance of its decision in order to consider whether the pen register evidence had been properly admitted at petitioner's trial. 283 Md. 156, 160, 389 A. 2d 858, 860 (1978).

The Court of Appeals affirmed the judgment of conviction, holding that "there is no constitutionally protected reasonable expectation of privacy in the numbers dialed into a telephone system and hence no search within the fourth amendment is implicated by the use of a pen register installed at the central offices of the telephone company." Id., at 173, 389 A. 2d, at 867. Because there was no "search," the court concluded, no warrant was needed. Three judges dissented, expressing the view that individuals do have a legitimate expectation of privacy regarding the phone numbers they dial from their homes; that the installation of a pen register thus constitutes a "search"; and that, in the absence of exigent circumstances, the failure of police to secure a warrant mandated that the pen register evidence here be excluded. Id., at 174, 178, 389 A. 2d, at 868, 870. Certiorari was granted in order to resolve indications of conflict in the decided cases as to the restrictions imposed by the Fourth Amendment on the use of pen registers. 3 439 U.S. 1001 (1978). [442 U.S. 735, 739]

II

A

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." In determining whether a particular form of government-initiated electronic surveillance is a "search" within the meaning of the Fourth Amendment, 4 our lodestar is Katz v. United States, 389 U.S. 347 (1967). In Katz, Government agents had intercepted the contents of a telephone conversation by attaching an electronic listening device to the outside of a public phone booth. The Court rejected the argument that a "search" can occur only when there has been a "physical intrusion" into a "constitutionally protected area," noting that the Fourth Amendment "protects people, not places." Id., at 351-353. Because the Government's monitoring of Katz' conversation "violated the privacy upon which he justifiably relied while using the telephone booth," the Court held that [442 U.S. 735, 740] it "constituted a `search and seizure' within the meaning of the Fourth Amendment." Id., at 353.

Consistently with Katz, this Court uniformly has held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a "justifiable," a "reasonable," or a "legitimate expectation of privacy" that has been invaded by government action. E. g., Rakas v. Illinois, 439 U.S. 128, 143 , and n. 12 (1978); id., at 150, 151 (concurring opinion); id., at 164 (dissenting opinion); United States v. Chadwick, 433 U.S. 1, 7 (1977); United States v. Miller, 425 U.S. 435, 442 (1976); United States v. Dionisio, 410 U.S. 1, 14 (1973); Couch v. United States, 409 U.S. 322, 335 -336 (1973); United States v. White, 401 U.S. 745, 752 (1971) (plurality opinion); Mancusi v. DeForte, 392 U.S. 364, 368 (1968); Terry v. Ohio, 392 U.S. 1, 9 (1968). This inquiry, as Mr. Justice Harlan aptly noted in his Katz concurrence, normally embraces two discrete questions. The first is whether the individual, by his conduct, has "exhibited an actual (subjective) expectation of privacy," 389 U.S., at 361 - whether, in the words of the Katz majority, the individual has shown that "he seeks to preserve [something] as private." Id., at 351. The second question is whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as `reasonable,'" id., at 361 - whether, in the words of the Katz majority, the individual's expectation, viewed objectively, is "justifiable" under the circumstances. Id., at 353. 5 See Rakas v. Illinois, 439 U.S., [442 U.S. 735, 741] at 143-144, n. 12; id., at 151 (concurring opinion); United States v. White, 401 U.S., at 752 (plurality opinion).

B

In applying the Katz analysis to this case, it is important to begin by specifying precisely the nature of the state activity that is challenged. The activity here took the form of installing and using a pen register. Since the pen register was installed on telephone company property at the telephone company's central offices, petitioner obviously cannot claim that his "property" was invaded or that police intruded into a "constitutionally protected area." Petitioner's claim, rather, is that, notwithstanding the absence of a trespass, the State, as did the Government in Katz, infringed a "legitimate expectation of privacy" that petitioner held. Yet a pen register differs significantly from the listening device employed in Katz, for pen registers do not acquire the contents of communications. This Court recently noted:

> "Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. These devices do not hear sound. They disclose only the telephone numbers that have been dialed - a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers." United States v. New York Tel. Co., 434 U.S. 159, 167 (1977). [442 U.S. 735, 742]

Given a pen register's limited capabilities, therefore, petitioner's argument that its installation and use constituted a "search" necessarily rests upon a claim that he had a "legitimate expectation of privacy" regarding the numbers he dialed on his phone.

This claim must be rejected. First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. In fact, pen registers and similar devices are routinely used by telephone companies "for the purposes of checking billing operations, detecting fraud, and preventing violations of law." United States v. New York Tel. Co., 434 U.S., at 174 -175. Electronic equipment is used not only to keep billing records of toll calls, but also "to keep a record of all calls dialed from a telephone which is subject to a special rate structure." Hodge v. Mountain States Tel. & Tel. Co., 555 F.2d 254, 266 (CA9 1977) (concurring opinion). Pen registers are regularly employed "to determine whether a home phone is being used to conduct a business, to check for a defective dial, or to check for overbilling." Note, The Legal Constraints upon the Use of the Pen Register as a Law Enforcement Tool, 60 Cornell L. Rev. 1028, 1029 (1975) (footnotes omitted). Although most people may be oblivious to a pen register's esoteric functions, they presumably have some awareness of one common use: to aid in the identification of persons making annoying or obscene calls. See, e. g., Von Lusch v. C & P Telephone Co., 457 F. Supp. 814, 816 (Md. 1978); Note, 60 Cornell L. Rev., at 1029-1030, n. 11; Claerhout, The Pen Register, 20 Drake L. Rev. 108, 110-111 (1970). Most phone books tell [442 U.S. 735, 743] subscribers, on a page entitled "Consumer Information," that the company "can frequently help in identifying to the authorities the origin of unwelcome and troublesome calls." E. g., Baltimore Telephone Directory 21 (1978); District of Columbia Telephone Directory 13 (1978). Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.

Petitioner argues, however, that, whatever the expectations of telephone users in general, he

demonstrated an expectation of privacy by his own conduct here, since he "us[ed] the telephone in his house to the exclusion of all others." Brief for Petitioner 6 (emphasis added). But the site of the call is immaterial for purposes of analysis in this case. Although petitioner's conduct may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed. Regardless of his location, petitioner had to convey that number to the telephone company in precisely the same way if he wished to complete his call. The fact that he dialed the number on his home phone rather than on some other phone could make no conceivable difference, nor could any subscriber rationally think that it would.

Second, even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not "one that society is prepared to recognize as `reasonable.'" Katz v. United States, 389 U.S., at 361 . This Court consistently has held that a person has no legitimate expectation of privacy in information he [442 U.S. 735, 744] voluntarily turns over to third parties. E. g., United States v. Miller, 425 U.S., at 442 -444; Couch v. United States, 409 U.S., at 335 -336; United States v. White, 401 U.S., at 752 (plurality opinion); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427 (1963). In Miller, for example, the Court held that a bank depositor has no "legitimate `expectation of privacy'" in financial information "voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business." 425 U.S., at 442 . The 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.

Because the depositor "assumed the risk" of disclosure, the Court held that it would be unreasonable for him to expect his financial records to remain private.

This analysis dictates that petitioner can claim no legitimate expectation of privacy here. 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. The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber. Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. Tr. of Oral Arg. 3-5, 11-12, 32. We [442 U.S. 735, 745] are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.

Petitioner argues, however, that automatic switching equipment differs from a live operator in one pertinent respect. An operator, in theory at least, is capable of remembering every number that is conveyed to him by callers. Electronic equipment, by contrast, can "remember" only those numbers it is programmed to record, and telephone companies, in view of their present billing practices, usually do not record local calls. Since petitioner, in calling McDonough, was making a local call, his expectation of privacy as to her number, on this theory, would be "legitimate."

This argument does not withstand scrutiny. The fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not, in our view, make any constitutional difference. Regardless of the phone company's election, petitioner voluntarily conveyed

to it information that it had facilities for recording and that it was free to record. In these circumstances, petitioner assumed the risk that the information would be divulged to police. Under petitioner's theory, Fourth Amendment protection would exist, or not, depending on how the telephone company chose to define local-dialing zones, and depending on how it chose to bill its customers for local calls. Calls placed across town, or dialed directly, would be protected; calls placed across the river, or dialed with operator assistance, might not be. We are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation.

We therefore conclude that petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not "legitimate." The installation and use of a pen register, [442 U.S. 735, 746] consequently, was not a "search," and no warrant was required. The judgment of the Maryland Court of Appeals is affirmed.

It is so ordered.

Mr. JUSTICE POWELL took no part in the consideration or decision of this case.

Footnotes

[Footnote 1] "A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed." United States v. New York Tel. Co., 434 U.S. 159, 161 n. 1 (1977). A pen register is "usually installed at a central telephone facility [and] records on a paper tape all numbers dialed from [the] line" to which it is attached. United States v. Giordano, 416 U.S. 505, 549 n. 1 (1974) (opinion concurring in part and dissenting in part). See also United States v. New York Tel. Co., 434 U.S., at 162 .

[Footnote 2] "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const., Amdt. 4.

[Footnote 3] See Application of United States for Order, 546 F.2d 243, 245 (CA8 1976), cert. denied sub nom. Southwestern Bell Tel. Co. v. United States, 434 U.S. 1008 (1978); Application of United States in Matter of Order, [442 U.S. 735, 739] 538 F.2d 956, 959-960 (CA2 1976), rev'd on other grounds sub nom. United States v. New York Tel. Co., 434 U.S. 159 (1977); United States v. Falcone, 505 F.2d 478, 482, and n. 21 (CA3 1974), cert. denied, 420 U.S. 955 (1975); Hodge v. Mountain States Tel. & Tel. Co., 555 F.2d 254, 256 (CA9 1977); id., at 266 (concurring opinion); and United States v. Clegg, 509 F.2d 605, 610 (CA5 1975). In previous decisions, this Court has not found it necessary to consider whether "pen register surveillance [is] subject to the requirements of the Fourth Amendment." United States v. New York Tel. Co., 434 U.S., at 165 n. 7. See United States v. Giordano, 416 U.S., at 554 n. 4 (opinion concurring in part and dissenting in part).

[Footnote 4] In this case, the pen register was installed, and the numbers dialed were recorded, by the telephone company. Tr. 73-74. The telephone company, however, acted at police request. Id., at 73, 75. In view of this, respondent appears to concede that the company is to be deemed an "agent" of the police for purposes of this case, so as to render the installation and use of the pen register "state action" under the Fourth and Fourteenth Amendments. We may assume that "state action" was present here.

[Footnote 5] Situations can be imagined, of course, in which Katz' two-pronged inquiry would provide an inadequate index of Fourth Amendment protection. For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects. Similarly, if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy [442 U.S. 735, 741] regarding the contents of his calls might be lacking as well. In such circumstances, where an individual's subjective expectations had been "conditioned" by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was. In determining whether a "legitimate expectation of privacy" existed in such cases, a normative inquiry would be proper.

Mr. JUSTICE STEWART, with whom MR. JUSTICE BRENNAN joins, dissenting.

I am not persuaded that the numbers dialed from a private telephone fall outside the constitutional protection of the Fourth and Fourteenth Amendments.

In Katz v. United States, 389 U.S. 347, 352 , the Court acknowledged the "vital role that the public telephone has come to play in private communication[s]." The role played by a private telephone is even more vital, and since Katz it has been abundantly clear that telephone conversations carried on by people in their homes or offices are fully protected by the Fourth and Fourteenth Amendments. As the Court said in United States v. United States District Court, 407 U.S. 297, 313 , "the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards." (Footnote omitted.)

Nevertheless, the Court today says that those safeguards do not extend to the numbers dialed from a private telephone, apparently because when a caller dials a number the digits may be recorded by the telephone company for billing purposes. But that observation no more than describes the basic nature of telephone calls. A telephone call simply cannot be made without the use of telephone company property and without payment to the company for the service. The telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment. Yet we [442 U.S. 735, 747] have squarely held that the user of even a public telephone is entitled "to assume that the words he utters into the mouthpiece will not be broadcast to the world." Katz v. United States, supra, at 352.

The central question in this case is whether a person who makes telephone calls from his home is entitled to make a similar assumption about the numbers he dials. What the telephone company does or might do with those numbers is no more relevant to this inquiry than it would be in a case involving the conversation itself. It is simply not enough to say, after Katz, that there is no legitimate expectation of privacy in the numbers dialed because the caller assumes the risk that the telephone company will disclose them to the police.

I think that the numbers dialed from a private telephone - like the conversations that occur during a call - are within the constitutional protection recognized in Katz. 1 It seems clear to me that information obtained by pen register surveillance of a private telephone is information in which the telephone subscriber has a legitimate expectation of privacy. 2 The information captured by such surveillance emanates from private conduct within a person's home or office - locations that without question are entitled to Fourth and Fourteenth Amendment protection. Further, that information is an integral part of

the telephonic communication that under Katz [442 U.S. 735, 748] is entitled to constitutional protection, whether or not it is captured by a trespass into such an area.

The numbers dialed from a private telephone - although certainly more prosaic than the conversation itself - are not without "content." Most private telephone subscribers may have their own numbers listed in a publicly distributed directory, but I doubt there are any who would be happy to have broadcast to the world a list of the local or long distance numbers they have called. This is not because such a list might in some sense be incriminating, but because it easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life.

I respectfully dissent.

[Footnote 1] It is true, as the Court pointed out in United States v. New York Tel. Co., 434 U.S. 159, 166 -167, that under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. 2510-2520, pen registers are not considered "interceptions" because "they do not acquire the `contents' of communications," as that term is defined by Congress. We are concerned in this case, however, not with the technical definitions of a statute, but with the requirements of the Constitution.

[Footnote 2] The question whether a defendant who is not a member of the subscriber's household has "standing" to object to pen register surveillance of a private telephone is, of course, distinct. Cf. Rakas v. Illinois, 439 U.S. 128 .

Mr. JUSTICE MARSHALL, with whom Mr. JUSTICE BRENNAN joins, dissenting.

The Court concludes that because individuals have no actual or legitimate expectation of privacy in information they voluntarily relinquish to telephone companies, the use of pen registers by government agents is immune from Fourth Amendment scrutiny. Since I remain convinced that constitutional protections are not abrogated whenever a person apprises another of facts valuable in criminal investigations, see, e. g., United States v. White, 401 U.S. 745, 786 -790 (1971) (Harlan, J., dissenting); id., at 795-796 (MARSHALL, J., dissenting); California Bankers Assn. v. Shultz, 416 U.S. 21, 95 -96 (1974) (MARSHALL, J., dissenting); United States v. Miller, 425 U.S. 435, 455 -456 (1976) (MARSHALL, J., dissenting), I respectfully dissent.

Applying the standards set forth in Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring), the Court first determines that telephone subscribers have no subjective expectations of privacy concerning the numbers they dial. To reach this conclusion, the Court posits that individuals somehow infer from the long-distance listings on their phone bills, and from the cryptic assurances of "help" in tracing obscene [442 U.S. 735, 749] calls included in "most" phone books, that pen registers are regularly used for recording local calls. See ante, at 742-743. But even assuming, as I do not, that individuals "typically know" that a phone company monitors calls for internal reasons, ante, at 743, 1 it does not follow that they expect this information to be made available to the public in general or the government in particular. Privacy 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. See California Bankers Assn. v. Shultz, supra, at 95-96 (MARSHALL, J., dissenting).

The crux of the Court's holding, however, is that whatever expectation of privacy petitioner may in fact have entertained regarding his calls, it is not one "society is prepared to recognize as `reasonable.'" Ante, at 743. In so ruling, the Court determines that individuals who convey information to third parties have "assumed the risk" of disclosure to the government. Ante, at 744, 745. This analysis is

misconceived in two critical respects.

Implicit in the concept of assumption of risk is some notion of choice. At least in the third-party consensual surveillance cases, which first incorporated risk analysis into Fourth Amendment doctrine, the defendant presumably had exercised some discretion in deciding who should enjoy his confidential communications. See, e. g., Lopez v. United States, 373 U.S. 427, 439 (1963); Hoffa v. United States, 385 U.S. 293, 302 -303 (1966); United States v. White, supra, at 751-752 [442 U.S. 735, 750] (plurality opinion). By contrast here, unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. Cf. Lopez v. United States, supra, at 465-466 (BRENNAN, J., dissenting). It is idle to speak of "assuming" risks in contexts where, as a practical mater, individuals have no realistic alternative.

More fundamentally, to make risk analysis dispositive in assessing the reasonableness of privacy expectations would allow the government to define the scope of Fourth Amendment protections. For example, law enforcement officials, simply by announcing their intent to monitor the content of random samples of first-class mail or private phone conversations, could put the public on notice of the risks they would thereafter assume in such communications. See Amsterdam, Perspectives on the Fourth Amendment, 58 Minn. L. Rev. 349, 384, 407 (1974). Yet, although acknowledging this implication of its analysis, the Court is willing to concede only that, in some circumstances, a further "normative inquiry would be proper." Ante, at 740-741, n. 5. No meaningful effort is made to explain what those circumstances might be, or why this case is not among them.

In my view, whether privacy expectations are legitimate within the meaning of Katz depends not on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society. By its terms, the constitutional prohibition of unreasonable searches and seizures assigns to the judiciary some prescriptive responsibility. As Mr. Justice Harlan, who formulated the standard the Court applies today, himself recognized: "[s]ince it is the task of the law to form and project, as well as mirror and reflect, we should not . . . merely recite . . . risks without examining the desirability of saddling them upon society." United States v. White, supra, at 786 (dissenting opinion). In making this [442 U.S. 735, 751] assessment, courts must evaluate the "intrinsic character" of investigative practices with reference to the basic values underlying the Fourth Amendment. California Bankers Assn. v. Shultz, 416 U.S., at 95 (MARSHALL, J., dissenting). And for those "extensive intrusions that significantly jeopardize [individuals'] sense of security . . ., more than self-restraint by law enforcement officials is required." United States v. White, 401 U.S., at 786 (Harlan, J., dissenting).

The use of pen registers, I believe, constitutes such an extensive intrusion. To hold otherwise ignores the vital role telephonic communication plays in our personal and professional relationships, see Katz v. United States, 389 U.S., at 352 , as well as the First and Fourth Amendment interests implicated by unfettered official surveillance. Privacy in placing calls is of value not only to those engaged in criminal activity. 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. See NAACP v. Alabama, 357 U.S. 449, 463 (1958); Branzburg v. Hayes, 408 U.S. 665, 695 (1972); id., at 728-734 (STEWART, J., dissenting). 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. Particularly given the Government's previous reliance on warrantless telephonic surveillance to trace reporters' sources and monitor protected political activity, 2 I am unwilling to insulate use of pen registers from independent judicial review. [442 U.S. 735, 752]

Just as one who enters a public telephone booth is "entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world," Katz v. United States, supra, at 352, so too, he should be entitled to assume that the numbers he dials in the privacy of his home will be recorded, if at all, solely for the phone company's business purposes. Accordingly, I would require law enforcement officials to obtain a warrant before they enlist telephone companies to secure information otherwise beyond the government's reach.

[Footnote 1] Lacking the Court's apparently exhaustive knowledge of this Nation's telephone books and the reading habits of telephone subscribers, see ante, at 742-743, I decline to assume general public awareness of how obscene phone calls are traced. Nor am I persuaded that the scope of Fourth Amendment protection should turn on the concededly "esoteric functions" of pen registers in corporate billing, ante, at 742, functions with which subscribers are unlikely to have intimate familiarity.

[Footnote 2] See, e. g., Reporters Committee For Freedom of Press v. American Tel. & Tel. Co., 192 U.S. App. D.C. 376, 593 F.2d 1030 (1978), cert. denied, 440 U.S. 949 (1979); Halperin v. Kissinger, 434 F. Supp. 1193 (DC 1977); Socialist Workers Party v. Attorney General, 463 F. Supp. 515 (SDNY 1978). [442 U.S. 735, 753]

United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued November 17, 2009 Decided August 6, 2010

No. 08-3030

UNITED STATES OF AMERICA,
APPELLEE

v.

LAWRENCE MAYNARD,
APPELLANT

GPS
Read 10/18

Consolidated with 08-3034

Appeals from the United States District Court
for the District of Columbia
(No. 1:05-cr-00386-ESH-10)

Sicilia C. Englert and *Stephen C. Leckar*, appointed by the court, argued the causes for appellants. With them on the briefs was *Michael E. Lawlor*.

David L. Sobel, *Daniel I. Prywes*, and *Arthur B. Spitzer* were on the brief for amici curiae American Civil Liberties Union of the National Capital Area and Electronic Frontier Foundation in support of appellant Jones.

Peter S. Smith, Assistant U.S. Attorney, argued the cause for appellee. With him on the brief were *Roy W. McLeese III*, *John V. Geise*, and *Rachel C. Lieber*, Assistant U.S. Attorneys.

Before: GINSBURG, TATEL and GRIFFITH, *Circuit Judges*.

Opinion for the Court filed by *Circuit Judge* GINSBURG.

GINSBURG, *Circuit Judge*: The appellants, Antoine Jones and Lawrence Maynard, appeal their convictions after a joint trial for conspiracy to distribute and to possess with intent to

distribute five kilograms or more of cocaine and 50 grams or more of cocaine base, in violation of 21 U.S.C. §§ 841 and 846. Maynard also challenges the sentence imposed by the district court. Because the appellants' convictions arise from the same underlying facts and they make several overlapping arguments, we consolidated their appeals. For the reasons that follow, we reverse Jones's and affirm Maynard's convictions.

I. Background

Jones owned and Maynard managed the "Levels" nightclub in the District of Columbia. In 2004 an FBI-Metropolitan Police Department Safe Streets Task Force began investigating the two for narcotics violations. The investigation culminated in searches and arrests on October 24, 2005. We discuss that investigation and the drug distribution operation it uncovered in greater detail where relevant to the appellants' arguments on appeal.

On October 25 Jones and several alleged co-conspirators were charged with, among other things, conspiracy to distribute and to possess with intent to distribute cocaine and cocaine base. Maynard, who was added as a defendant in superseding indictments filed in March and June 2006, pled guilty in June 2006.

In October 2006 Jones and a number of his co-defendants went to trial. The jury acquitted the co-defendants on all counts but one; it could not reach a verdict on the remaining count, which was eventually dismissed. The jury acquitted Jones on a number of counts but could not reach a verdict on the conspiracy charge, as to which the court declared a mistrial. Soon thereafter the district court allowed Maynard to withdraw his guilty plea.

In March 2007 the Government filed another superseding indictment charging Jones, Maynard, and a few co-defendants with a single count of conspiracy to distribute and to possess with intent to distribute five or more kilograms of cocaine and 50 or more grams of cocaine base. A joint trial of Jones and Maynard began in November 2007 and ended in January 2008, when the jury found them both guilty.

II. Analysis: Joint Issues

Jones and Maynard jointly argue the district court erred in (1) admitting evidence gleaned from wiretaps of their phones, (2) admitting evidence arising from a search incident to a traffic stop, (3) denying their motion to dismiss the indictment as invalid because it was handed down by a grand jury that had expired, (4) declining to instruct the jury on their theory that the evidence at trial suggested multiple conspiracies, and (5) declining to grant immunity to several defense witnesses who invoked the Fifth Amendment to the Constitution of the United States and refused to testify. Jones also argues the court erred in admitting evidence acquired by the warrantless use of a Global Positioning System (GPS) device to track his movements continuously for a month.* After concluding none of the joint issues warrants reversal, we turn to Jones's individual argument.

---

* Maynard waves at one individual argument, to wit, that "the district court erred in using acquitted conduct to calculate his guideline range" but, in the same sentence, concedes his argument "is foreclosed by" precedent, *e.g.*, *United States v. Dorcely*, 454 F.3d 366 (D.C. Cir. 2006) (district court's consideration of prior acquitted conduct did not violate the Fifth or Sixth Amendments to the Constitution of the United States). He nonetheless "raises this issue to preserve his argument in anticipation of future changes in the law and/or *en banc* review." So be it.

A. Wiretaps

Before their first trial Jones and his co-defendants moved to suppress evidence taken from wiretaps on Jones's and Maynard's phones. The police had warrants for the wiretaps, but the defendants argued the issuing court abused its discretion in approving the warrants because the applications for the warrants did not satisfy the so-called "necessity requirement," *see* 18 U.S.C. § 2518(3)(c) ("normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous"); *see also, e.g.*, *United States v. Becton*, 601 F.3d 588, 596 (D.C. Cir. 2010). They also moved for a hearing, pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), into the credibility of one of the affidavits offered in support of the warrant. The district court denied both motions. 451 F. Supp. 2d 71, 78–79, 81–83 (2006). Before his second trial Jones moved the court to reconsider both motions; Maynard adopted Jones's motions and made an additional argument for a *Franks* hearing. The district court held Jones's motion for reconsideration added nothing new and denied it for the reasons the court had given before the first trial. 511 F. Supp. 2d 74, 77 (2007). The court then denied Maynard's separate motion for a *Franks* hearing. *Id.* at 78. The appellants appeal the district court's denial of their motions to suppress and for a *Franks* hearing.

As for their motions to suppress, the district court held the applications for the warrants "amply satisfie[d]" the necessity requirement because they recounted the ordinary investigative procedures that had been tried and explained why wiretapping was necessary in order to "ascertain the extent and structure of the conspiracy." 451 F. Supp. 2d at 83. We review the court's "necessity determination" for

abuse of discretion. *United States v. Sobamowo*, 892 F.2d 90, 93 (D.C. Cir. 1989).

The appellants do not directly challenge the reasoning of the district court; rather they suggest sources of information to which the police hypothetically might have turned in lieu of the wiretaps, to wit, cooperating informants, controlled buys, and further video surveillance. At best, the appellants suggest investigative techniques that might have provided some of the evidence needed, but they give us no reason to doubt the district court's conclusion that "[h]aving engaged in an adequate range of investigative endeavors, the government properly sought wiretap permission and was not required to enumerate every technique or opportunity missed or overlooked." 451 F. Supp. 2d at 82 (quoting *Sobamowo*, 892 F.2d at 93).

The appellants also requested a hearing into the credibility of the affidavit submitted by Special Agent Yanta in support of the wiretap warrants. An affidavit offered in support of a search warrant enjoys a "presumption of validity," *Franks*, 438 U.S. at 171, but

> where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request.

Id. at 155–56. The substantial showing required under *Franks* must be "more than conclusory" and "accompanied by an offer of proof." *United States v. Gatson*, 357 F.3d 77, 80 (D.C. Cir. 2004) (quoting *Franks*).

The appellants argued Yanta intentionally or at least recklessly both mischaracterized certain evidence and omitted any mention in her affidavit of Holden, an informant whom the appellants think might have assisted the investigation. The district court denied the motion, holding the appellants had satisfied neither the substantial showing nor the materiality requirement for a *Franks* hearing. 451 F. Supp. 2d at 78–79; 511 F. Supp. 2d at 77–78.

As we recently noted, "[t]he circuits are split on the question whether a district court's decision not to hold a *Franks* hearing is reviewed under the clearly erroneous or *de novo* standard of review," and "[w]e have not definitively resolved the issue in this circuit." *United States v. Becton*, 601 F.3d 588, 594 (2010) (internal quotation marks deleted). We need not resolve the issue today because even proceeding *de novo* we would agree with the district court: The appellants did not make the requisite substantial preliminary showing that Yanta, in her affidavit, intentionally or recklessly either described the evidence in a misleading way or failed to mention Holden. Lacking any probative evidence of Yanta's *scienter*, the appellants argue the district court should have inferred Yanta knew about Holden and intentionally failed to mention him because his name must have "flashed across the Task Force's team computer screens." This is speculation, not a substantial showing, and no basis upon which to question the ruling of the district court. *See United States v. Richardson*, 861 F.2d 291, 293 (D.C. Cir. 1988) (affidavit in support of warrant not suspect under *Franks* where "there has been absolutely no showing [the affiant] made the statements with scienter").

B. Traffic Stop

In 2005 Officer Frederick Whitehead, of the Durham, North Carolina Police Department, pulled over Jones's mini-van for speeding. Because we consider the "evidence in the light most favorable to the Government," *Evans v. United States*, 504 U.S. 255, 257 (1992), what follows is the Officer's account of the incident.

Maynard was driving and one Gordon was asleep in the passenger seat; Jones was not present. At the officer's request Maynard walked to the rear of the vehicle. There, in response to Whitehead's questioning, Maynard said he worked for a nightclub in D.C. and was driving to South Carolina to pick up a disc jockey and to bring him back for an event. When asked about his passenger, Maynard claimed not to know Gordon's last name or age. Whitehead then addressed Gordon, who had awakened and whom he thought seemed nervous, and asked him where he was going. Gordon told a different story: He and Maynard were headed to Georgia in order to meet relatives and some girls.

Whitehead then went to speak with his partner, who had arrived in a separate car. After relating the suspicious conflict in the stories he had been told, Whitehead called for a canine unit and ran the usual checks on Maynard's license and registration. He then returned to the rear of the van, where Maynard was still standing, gave Maynard back his identification, along with a warning citation, and told him he was free to leave. By that time, the canine unit had arrived on scene but remained in their vehicle. Maynard moved toward the front of the van and, as he reached to open the driver's-side door, Whitehead called out "do you mind if I ask you a few additional questions?" Maynard turned around and walked back toward Whitehead, who then asked him if he

was transporting any large sums of money, illegal weapons, or explosives. Maynard "looked scared," said nothing, closed his eyes, and held his breath. He then looked at the rear of the van, told Whitehead he had a cooler he had meant to put some ice in, and reached toward the rear latch. Whitehead said not to open the door and asked Maynard if he would consent to a search; when Maynard said "yes," Whitehead frisked Maynard for weapons, asked Gordon to step out of the vehicle, frisked him for weapons, and then gave the canine unit the go-ahead. The dog alerted while sniffing around the car, and the ensuing search of the van turned up $69,000 in cash.

Before trial the appellants moved unsuccessfully to suppress evidence from the traffic stop, arguing, as they do now, that by extending the traffic stop after giving Maynard his written warning the police (1) unreasonably seized Maynard, *see Illinois v. Caballes*, 543 U.S. 405, 407–08 (2005) ("A seizure that is justified solely by the interest in issuing a warning ticket to the driver can become unlawful if it is prolonged beyond the time reasonably required to complete that mission"), and (2) unreasonably searched the van, all in violation of the Fourth Amendment to the Constitution of the United States. The district court held the extended stop was not a seizure because Maynard was free to leave and, if it was a seizure, then it was lawful because it was supported by reasonable suspicion. As for the search of the van, the district court held the canine sniff was not a search and, once the canine alerted, the police had probable cause to search the vehicle. "We consider a district court's legal rulings on a suppression motion *de novo* and review its factual findings for clear error giving due weight to inferences drawn from those facts and its determination of witness credibility." *United States v. Holmes*, 505 F.3d 1288, 1292 (D.C. Cir. 2007) (internal quotation marks deleted).

he said yes

is that a search?

In determining whether a person has been seized within the meaning of the Fourth Amendment, "the appropriate inquiry is whether a reasonable person would feel free to decline the officers' requests or otherwise terminate the encounter." *Florida v. Bostick*, 501 U.S. 429, 436 (1991). This inquiry "tak[es] into account all of the circumstances surrounding the encounter," *id.*, in the light of which we ask "not whether the citizen [in this case] perceived that he was being ordered to restrict his movement, but whether the officer's words and actions would have conveyed that [message] to a reasonable person," *California v. Hodari D.*, 499 U.S. 621, 628 (1991). So it is that "[a] stop or seizure takes place only when the officer, by means of physical force or show of authority, has in some way restrained the liberty of a citizen." *United States v. Jones*, 584 F.3d 1083, 1086 (D.C. Cir. 2009) (internal quotation marks omitted); *see also* David K. Kessler, *Free to Leave? An Empirical Look at the Fourth Amendment's Seizure Standard*, 99 J. Crim. L. & Criminology 51, 60 (2009) ("The Court has declined to find seizures based on mere interaction with law enforcement without a showing of some degree of outward coercion"). Whether a seizure has taken place "is a legal conclusion that this court reviews *de novo*." *United States v. Jordan*, 958 F.2d 1085, 1086 (D.C. Cir. 1992).

The appellants argue Maynard was seized because, when Officer Whitehead told Maynard he was free to go, he "had already decided that he was going to search the van .... Whitehead had no intention of letting him go until after he [had searched it]." This assertion, even if true, has no bearing upon whether a reasonable person would have felt free to decline Whitehead's request. That Maynard seemed nervous when Whitehead asked him whether he was carrying any contraband or large sums of money, which Maynard offers as

further evidence he was "under duress," is irrelevant for the same reason.

We agree with the district court that, considering all the circumstances surrounding the stop, a reasonable person in Maynard's position would have felt free to decline Whitehead's request that he answer "a few additional questions." *See United States v. Wylie*, 569 F.2d 62, 67 (D.C. Cir. 1977) ("police-citizen communications which take place under circumstances in which the citizen's 'freedom to walk away' is not limited by anything other than his desire to cooperate do not amount to 'seizures' of the person"). Whitehead had already returned Maynard's license and registration and told him he was free to go. Although there were by that time three police cars (two of which were unmarked) on the scene, Whitehead's words and actions unambiguously conveyed to Maynard his detention was at an end. After that, Maynard returned to the front of the van — a clear sign he thought he was free to go. By remaining behind the vehicle as Maynard left, Whitehead further assured Maynard he would not impede his leaving. Finally, Maynard turned around and came back only when Whitehead re-initiated the stop by asking him if he would answer a few more questions. That Whitehead shouted the question might in some circumstances turn it into a show of authority, but not here; the two were standing some distance apart on the side of a noisy interstate highway. In sum, the police did not seize Maynard by asking him whether he would answer a few more questions.

The appellants' brief might be read to argue the extension of the stop, from the time Whitehead frisked Maynard until the dog alerted, was a separate seizure. *See United States v. Alexander*, 448 F.3d 1014, 1016 (8th Cir. 2006) (dog sniff "may be the product of an unconstitutional seizure [] if the

traffic stop is unreasonably prolonged before the dog is employed"). If Maynard's and Gordon's inconsistent statements, Maynard's claimed lack of knowledge about Gordon, and Gordon's nervousness had not already created "reasonable suspicion to believe that criminal activity [was] afoot," *United States v. Arvizu*, 534 U.S. 266, 273 (2002) (internal quotation marks deleted), however, then surely the addition of Maynard's agitated reaction to Whitehead's renewed questioning did, *see Illinois v. Wardlow*, 528 U.S. 119, 123 (2000) ("nervous, evasive behavior is a pertinent factor in determining reasonable suspicion").

The parties also dispute whether Maynard's consent to the search of the van was voluntary and whether Jones has standing to challenge that search. Those issues are mooted by our holding the extension of the stop to ask Maynard a few additional questions was not a seizure and any subsequent extension of the stop leading up to the canine sniff was supported by reasonable suspicion. The appellants do not dispute the district court's determination that the police had probable cause to search the van once the dog alerted. Accordingly, we hold the district court properly admitted evidence the police discovered by searching the van.

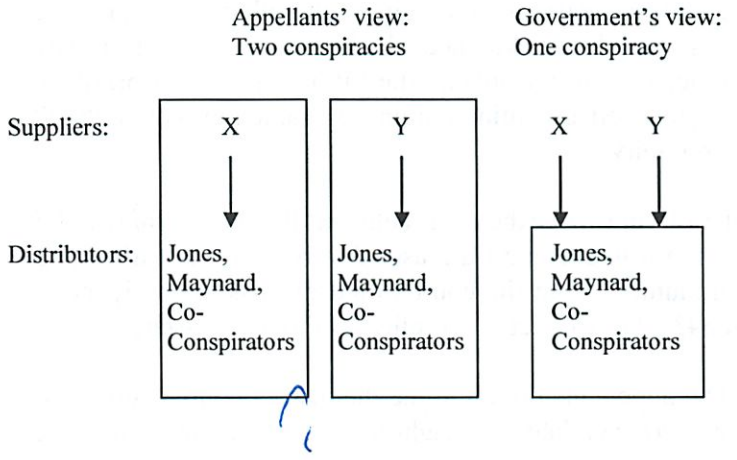
C. Superseding Indictment

The appellants argue the indictment returned June 27, 2006 was invalid because it was returned by a grand jury whose term had expired. As the Government points out, the validity of that indictment is irrelevant here because the appellants were charged and tried pursuant to the superseding indictment returned by a different grand jury on March 21, 2007. The appellants point to no infirmity in the relevant indictment.

D. Multiple Conspiracies

At trial the appellants asked the court to instruct the jury that proof of multiple separate conspiracies is not proof of one larger conspiracy. The district court denied that request, which the appellants argue was reversible error under *United States v. Graham*, 83 F.3d 1466, 1472 (D.C. Cir. 1996): "To convict, the jury must find appellants guilty of the conspiracy charged in the indictment, not some other, separate conspiracy"; therefore, "if record evidence supports the existence of multiple conspiracies, the district court should ... so instruct[] the jury."

The appellants argue the evidence at trial supports the existence of "[t]wo independent supply-side conspiracies." The two purportedly separate conspiracies they instance, however, each comprises the core conspiracy charged — that of Maynard, Jones, and the same co-conspirators, to possess and to distribute cocaine and cocaine base — differing only as to the supplier of the drugs, as reflected in the following illustration:



Even if the evidence showed the charged conspiracy to distribute drugs relied upon two different suppliers, and the Government does not concede it did, that does not cleave in two the single conspiracy to distribute the appellants were charged with operating. As the appellants offer no other reason to doubt the district court's conclusion, in rejecting the proposed instruction, that "[t]he defendants here and their coconspirators [were] involved in a single overarching conspiracy," there was no error in the district court's refusal to instruct the jury about multiple conspiracies.

E. Immunity

At trial, the appellants called a number of their co-conspirators as witnesses, but the co-conspirators refused to testify, asserting their right, under the Fifth Amendment, not to be compelled to incriminate themselves. The appellants then asked the district court, "in its discretion, [to] adopt [the] rationale and ... procedure" set forth in *Carter v. United States*, 684 A.2d 331 (1996), where the District of Columbia Court of Appeals addressed a situation in which

> a defense witness possessing material, exculpatory and non-cumulative evidence which is unobtainable from any other source will invoke the Fifth Amendment privilege against self-incrimination unless granted executive "use" immunity.

Id. at 342. In *Carter* the court held that if the Government did not "submit to the court a reasonable basis for not affording use immunity," then the court would dismiss the indictment. *Id.* at 343. The district court refused to follow *Carter*.

The appellants do not argue the district court's refusal to follow *Carter* violated any right they had under any source of

law. The closest they come is to say "a strong case can be made that [use immunity] is compelled ... by due process considerations," but they do not make any effort to show this case presents the sort of "extraordinary circumstances" in which some courts have suggested the Government's failure to grant use immunity might violate the Due Process Clause of the Fifth Amendment, *see, e.g.*, *United States v. Pinto*, 850 F.2d 927, 935 (2d Cir. 1988) (discussing three-part test used to determine whether failure of Government to grant immunity violates due process, including "prosecutorial overreaching"); *cf. United States v. Lugg*, 892 F.2d 101, 104 (D.C. Cir. 1989) (reserving due process issue: "[w]hatever it takes to constitute a deprivation of a fair trial by the prosecution's failure to exercise its broad discretion on immunity grants, the present case does not present it").

Instead, their counsel told the district court:

> I'll be straight. I'll be honest with the Court. I don't believe that there's any case law in this jurisdiction or another federal jurisdiction that would allow the Court to do this. ... I think that the Court should, in its discretion, adopt [the rule in *Carter*].

The appellants mistake our role in asking us "to fashion[]" a rule of the sort the district court declined to adopt. Absent a well-founded claim they were deprived of due process, the only question they may properly raise is whether the district court abused its discretion, to which the answer is obviously no.

III. Analysis: Evidence Obtained from GPS Device

Jones argues his conviction should be overturned because the police violated the Fourth Amendment prohibition of

"unreasonable searches" by tracking his movements 24 hours a day for four weeks with a GPS device they had installed on his Jeep without a valid warrant.* We consider first whether that use of the device was a search and then, having concluded it was, consider whether it was reasonable and whether any error was harmless.

A. Was Use of GPS a Search?

For his part, Jones argues the use of the GPS device violated his "reasonable expectation of privacy," *United States v. Katz*, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring), and was therefore a search subject to the reasonableness requirement of the Fourth Amendment. Of course, the Government agrees the *Katz* test applies here, but it argues we need not consider whether Jones's expectation of privacy was reasonable because that question was answered in *United States v. Knotts*, 460 U.S. 276 (1983), in which the Supreme Court held the use of a beeper device to aid in tracking a suspect to his drug lab was not a search. As explained below, we hold *Knotts* does not govern this case and the police action was a search because it defeated Jones's reasonable expectation of privacy. We then turn to the Government's claim our holding necessarily implicates prolonged visual surveillance.

---

* Although the Jeep was registered in the name of Jones's wife, the Government notes "Jones was the exclusive driver of the Jeep," and does not argue his non-ownership of the Jeep defeats Jones's standing to object. We see no reason it should. *See Rakas v. Illinois*, 439 U.S. 128, 148–49 & n.17 (1978) (whether defendant may challenge police action as search depends upon his legitimate expectation of privacy, not upon his legal relationship to the property searched). We therefore join the district court and the parties in referring to the Jeep as being Jones's. 451 F. Supp. 2d 71, 87 (2006).

wife has nothing to do w/ it

1. *Knotts* is not controlling

The Government argues this case falls squarely within the holding in *Knotts* that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." 460 U.S. at 281. In that case the police had planted a beeper in a five-gallon container of chemicals before it was purchased by one of Knotts's co-conspirators; monitoring the progress of the car carrying the beeper, the police followed the container as it was driven from the "place of purchase, in Minneapolis, Minnesota, to [Knotts's] secluded cabin near Shell Lake, Wisconsin," 460 U.S. at 277, a trip of about 100 miles. Because the co-conspirator, by driving on public roads, "voluntarily conveyed to anyone who wanted to look" his progress and route, he could not reasonably expect privacy in "the fact of his final destination." *Id.* at 281.

The Court explicitly distinguished between the limited information discovered by use of the beeper — movements during a discrete journey — and more comprehensive or sustained monitoring of the sort at issue in this case. *Id.* at 283 (noting "limited use which the government made of the signals from this particular beeper"); *see also id.* at 284–85 ("nothing in this record indicates that the beeper signal was received or relied upon after it had indicated that the [container] had ended its automotive journey at rest on respondent's premises in rural Wisconsin"). Most important for the present case, the Court specifically reserved the question whether a warrant would be required in a case involving "twenty-four hour surveillance," stating

> if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.

Id. at 283–84.

what is reasonable for privacy?

Although the Government, focusing upon the term "dragnet," suggests *Knotts* reserved the Fourth Amendment question that would be raised by mass surveillance, not the question raised by prolonged surveillance of a single individual, that is not what happened. In reserving the "dragnet" question, the Court was not only addressing but in part actually quoting the defendant's argument that, if a warrant is not required, then prolonged "twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision." *Id.* at 283.* The

* Indeed, the quoted section of the respondent's brief envisions a case remarkably similar to the one before us:

> We respectfully submit that the Court should remain mindful that should it adopt the result maintained by the government, twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision. Without the limitations imposed by the warrant requirement itself, and the terms of any warrant which is issued, any person or residence could be monitored at any time and for any length of time. Should a beeper be installed in a container of property which is not contraband, as here, it would enable authorities to determine a citizen's location at any time without knowing whether his travels are for legitimate or illegitimate purposes, should the container be moved. A beeper thus would turn a person into a broadcaster of his own affairs and travels, without his knowledge or consent, for as long as the government may wish to use him where no warrant places a limit on surveillance. To allow warrantless beeper monitoring,

Court avoided the question whether prolonged "twenty-four hour surveillance" was a search by limiting its holding to the facts of the case before it, as to which it stated "the reality hardly suggests abuse." *Id.* at 283 (internal quotation marks deleted).

In short, *Knotts* held only that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another," *id.* at 281, not that such a person has no reasonable expectation of privacy in his movements whatsoever, world without end, as the Government would have it. The Fifth Circuit likewise has recognized the limited scope of the holding in *Knotts*, *see United States v. Butts*, 729 F.2d 1514, 1518 n.4 (1984) ("As did the Supreme Court in *Knotts*, we pretermit any ruling on worst-case situations that may involve persistent, extended, or unlimited violations of a warrant's terms"), as has the New York Court of Appeals, *see People v. Weaver*, 12 N.Y.3d 433, 440–44 (2009) (*Knotts* involved a "single trip" and Court "pointedly acknowledged and reserved for another day the question of whether a Fourth Amendment issue would be posed if 'twenty-four hour surveillance of any citizen of this country [were] possible'"). *See also* Renee McDonald Hutchins, *Tied Up in Knotts? GPS Technology and the Fourth Amendment*, 419 UCLA L. Rev. 409, 457 (2007) ("According to the [Supreme] Court, its decision [in *Knotts*] should not be read to sanction 'twenty-four hour surveillance of any citizen of this country.'" (quoting *Knotts*, 460 U.S. at 284)).

---

particularly under the standard urged by the government here ("reasonable suspicion"), would allow virtually limitless intrusion into the affairs of private citizens.

Br. of Resp. at 9–10 (No. 81-1802).

Two circuits, relying upon *Knotts*, have held the use of a GPS tracking device to monitor an individual's movements in his vehicle over a prolonged period is not a search, *United States v. Pineda-Moreno*, 591 F.3d 1212 (9th Cir. 2010); *United States v. Garcia*, 474 F.3d 994 (7th Cir. 2007), but in neither case did the appellant argue that *Knotts* by its terms does not control whether prolonged surveillance is a search, as Jones argues here. Indeed, in *Garcia* the appellant explicitly conceded the point. Br. of Appellant at 22 (No. 06-2741) ("Garcia does not contend that he has a reasonable expectation of privacy in the movements of his vehicle while equipped with the GPS tracking device as it made its way through public thoroughfares. *Knotts*. His challenge rests solely with whether the warrantless installation of the GPS device, in and of itself, violates the Fourth Amendment."). Thus prompted, the Seventh Circuit read *Knotts* as blessing all "tracking of a vehicle on public streets" and addressed only "whether installing the device in the vehicle converted the subsequent tracking into a search." *Garcia*, 474 F.3d at 996. The court viewed use of a GPS device as being more akin to hypothetical practices it assumed are not searches, such as tracking a car "by means of cameras mounted on lampposts or satellite imaging," than it is to practices the Supreme Court has held are searches, such as attaching a listening device to a person's phone. *Id.* at 997. For that reason it held installation of the GPS device was not a search. Similarly, the Ninth Circuit perceived no distinction between short- and long-term surveillance; it noted the appellant had "acknowledged" *Knotts* controlled the case and addressed only whether *Kyllo v. United States*, 533 U.S. 27 (2001), in which the Court held the use of a thermal imaging device to detect the temperature inside a home defeats the occupant's reasonable expectation of privacy, had "heavily modified the Fourth Amendment analysis." *Pineda-Moreno*, 591 F.3d at 1216.

In a third related case the Eighth Circuit held the use of a GPS device to track a truck used by a drug trafficking operation was not a search. *United States v. Marquez*, 605 F.3d 604 (2010). After holding the appellant had no standing to challenge the use of the GPS device, the court went on to state in the alternative:

> Even if Acosta had standing, we would find no error. ... [W]hen police have reasonable suspicion that a particular vehicle is transporting drugs, a warrant is not required when, while the vehicle is parked in a public place, they install a non-invasive GPS tracking device on it for a reasonable period of time.

Id. at 609–10.

In each of these three cases the court expressly reserved the issue it seems to have thought the Supreme Court had reserved in *Knotts*, to wit, whether "wholesale" or "mass" electronic surveillance of many individuals requires a warrant. *Marquez*, 605 F.3d at 610; *Pineda-Moreno*, 591 F.3d at 1216 n.2; *Garcia*, 474 F.3d at 996. As we have explained, in *Knotts* the Court actually reserved the issue of prolonged surveillance. That issue is squarely presented in this case. Here the police used the GPS device not to track Jones's "movements from one place to another," *Knotts*, 460 U.S. at 281, but rather to track Jones's movements 24 hours a day for 28 days as he moved among scores of places, thereby discovering the totality and pattern of his movements from place to place to place.

2. Were Jones's locations exposed to the public?

As the Supreme Court observed in *Kyllo*, the "*Katz* test — whether the individual has an expectation of privacy that

society is prepared to recognize as reasonable — has often been criticized as circular, and hence subjective and unpredictable." 533 U.S. at 34. Indeed, the Court has invoked various and varying considerations in applying the test. *See O'Connor v. Ortega*, 480 U.S. 709, 715 (1987) ("We have no talisman that determines in all cases those privacy expectation that society is prepared to accept as reasonable") (O'Connor, J., plurality opinion); *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978) ("legitimation of expectations of privacy must have a source outside the Fourth Amendment," such as "understandings that are recognized or permitted by society"). This much is clear, however: Whether an expectation of privacy is reasonable depends in large part upon whether that expectation relates to information that has been "expose[d] to the public," *Katz*, 389 U.S. at 351.

Two considerations persuade us the information the police discovered in this case — the totality of Jones's movements over the course of a month — was not exposed to the public: First, unlike one's movements during a single journey, the whole of one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively nil. Second, the whole of one's movements is not exposed *constructively* even though each individual movement is exposed, because that whole reveals more — sometimes a great deal more — than does the sum of its parts.

a. Actually exposed?

The holding in *Knotts* flowed naturally from the reasoning in *Katz*: "What a person knowingly exposes to the public ... is not a subject of Fourth Amendment protection," 389 U.S. at 351. *See Knotts*, 460 U.S. at 281–82 (movements observed by police were "voluntarily conveyed to anyone

who wanted to look"). The Government argues the same reasoning applies here as well. We first consider the precedent governing our analysis of whether the subject of a purported search has been exposed to the public, then hold the information the police discovered using the GPS device was not so exposed.

(i). Precedent

The Government argues Jones's movements over the course of a month were actually exposed to the public because the police lawfully could have followed Jones everywhere he went on public roads over the course of a month. The Government implicitly poses the wrong question, however.

In considering whether something is "exposed" to the public as that term was used in *Katz* we ask not what another person can physically and may lawfully do but rather what a reasonable person expects another might actually do. *See California v. Greenwood*, 486 U.S. 35, 40 (1988) ("It is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public"); *California v. Ciraolo*, 476 U.S. 207, 213, 214 (1986) ("in an age where private and commercial flight in the public airways is routine," defendant did not have a reasonable expectation of privacy in location that "[a]ny member of the public flying in this airspace who glanced down could have seen"); *Florida v. Riley*, 488 U.S. 445, 450 (1989) ("Here, the inspection was made from a helicopter, but as is the case with fixed-wing planes, 'private and commercial flight [by helicopter] in the public airways is routine' in this country, and there is no indication that such flights are unheard of in Pasco County, Florida" (quoting *Ciraolo*)). Indeed, in *Riley*,

Justice O'Connor, whose concurrence was necessary to the judgment, pointed out:

> Ciraolo's expectation of privacy was unreasonable not because the airplane was operating where it had a "right to be," but because public air travel at 1,000 feet is a sufficiently routine part of modern life that it is unreasonable for persons on the ground to expect that their curtilage will not be observed from the air at that altitude.
>
> ....
>
> If the public rarely, if ever, travels overhead at such altitudes, the observation cannot be said to be from a vantage point generally used by the public and Riley cannot be said to have "knowingly expose[d]" his greenhouse to public view.

488 U.S. at 453, 455; *see also id.* at 467 (Blackmun, J., dissenting) (explaining five justices agreed "the reasonableness of Riley's expectation depends, in large measure, on the frequency of nonpolice helicopter flights at an altitude of 400 feet").

The Supreme Court re-affirmed this approach in *Bond v. United States*, 529 U.S. 334 (2000). There a passenger on a bus traveling to Arkansas from California had placed his soft luggage in the overhead storage area above his seat. During a routine stop at an off-border immigration checkpoint in Sierra Blanca, Texas, a Border Patrol agent squeezed the luggage in order to determine whether it contained drugs and thus detected a brick of what turned out to be methamphetamine. The defendant argued the agent had defeated his reasonable expectation of privacy, and the Government argued his

expectation his bag would not be squeezed was unreasonable because he had exposed it to the public. The Court responded:

> [A] bus passenger clearly expects that his bag may be handled. He does not expect that other passengers or bus employees will, as a matter of course, feel the bag in an exploratory manner. But this is exactly what the agent did here. We therefore hold that the agent's physical manipulation of petitioner's bag violated the Fourth Amendment.

Id. at 338–39. The Court focused not upon what other passengers could have done or what a bus company employee might have done, but rather upon what a reasonable bus passenger expects others he may encounter, i.e., fellow passengers or bus company employees, might actually do. A similar focus can be seen in *Kyllo*, in which the Court held use of a thermal imaging device defeats the subject's reasonable expectation of privacy, "at least where ... the technology in question is not in general public use." 533 U.S. at 34.

The Government cites as authority to the contrary our statement in *United States v. Gbemisola*, 225 F.3d 753, 759 (2000), that "[t]he decisive issue ... is not what the officers saw but what they could have seen." When read in context, however, this snippet too supports the view that whether something is "expose[d] to the public," *Katz*, 389 U.S. at 351, depends not upon the theoretical possibility, but upon the actual likelihood, of discovery by a stranger:

> The decisive issue ... is not what the officers saw but what they could have seen. At any time, the surveillance vehicle could have pulled alongside of the taxi and the

> officers could have watched Gbemisola through its window. Indeed, the taxi driver himself could have seen the event simply by looking in his rear-view mirror or turning around. As one cannot have a reasonable expectation of privacy concerning an act performed within the visual range of a complete stranger, the Fourth Amendment's warrant requirement was not implicated.

225 F.3d at 759. In short, it was not at all unlikely Gbemisola would be observed opening a package while seated in the rear of a taxi, in plain view of the driver and perhaps of others.

(ii). Application

Applying the foregoing analysis to the present facts, we hold the whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil. It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's hitherto private routine.

b. Constructively exposed?

The Government does not separately raise, but we would be remiss if we did not address, the possibility that although the whole of Jones's movements during the month for which the police monitored him was not actually exposed to the public, it was constructively exposed because each of his individual movements during that time was itself in public

view. When it comes to privacy, however, precedent suggests that the whole may be more revealing than the parts. Applying that precedent to the circumstances of this case, we hold the information the police discovered using the GPS device was not constructively exposed.

(i). Precedent

The Supreme Court addressed the distinction between a whole and the sum of its parts in *United States Department of Justice v. National Reporters Committee*, 489 U.S. 749 (1989), which arose not under the Fourth Amendment but under the Freedom of Information Act, 5 U.S.C. § 552. There the respondents had requested, pursuant to the FOIA, that the FBI disclose rap sheets compiling the criminal records of certain named persons. Although the "individual events in those summaries [were] matters of public record," the Court upheld the FBI's invocation of the privacy exception to the FOIA, holding the subjects had a privacy interest in the aggregated "whole" distinct from their interest in the "bits of information" of which it was composed. *Id.* at 764.* Most relevant to the Fourth Amendment, the Court said disclosure of a person's rap sheet "could reasonably be expected to constitute an unwarranted invasion of personal privacy." *Id.*

Wow - really

The Court implicitly recognized the distinction between the whole and the sum of the parts in the Fourth Amendment case of *Smith v. Maryland*, 442 U.S. 735 (1979). There, in holding the use of a pen register to record all the numbers

* The colloquialism that "the whole is greater than the sum of its parts" is not quite correct. "It is more correct to say that the whole is something different than the sum of its parts." Kurt Koffka, Principles of Gestalt Psychology 176 (1935). That is what the Court was saying in *Reporters Committee* and what we mean to convey throughout this opinion.

dialed from a person's phone was not a search, the Court considered not just whether a reasonable person expects any given number he dials to be exposed to the phone company but also whether he expects all the numbers he dials to be compiled in a list. *Id.* at 742–43 ("subscribers realize ... the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills"; they "typically know that ... the phone company has facilities for recording" the numbers they dial). The Court explained that Smith could not reasonably expect privacy in the list of numbers because that list was composed of information that he had "voluntarily conveyed to [the company]" and that "it had facilities for recording and ... was free to record." *Id.* at 745.

if cas have GPS for day that send to car company - expectation they won't

If, for the purposes of the Fourth Amendment, the privacy interest in a whole could be no greater (or no different) than the privacy interest in its constituent parts, then the Supreme Court would have had no reason to consider at length whether Smith could have a reasonable expectation of privacy in the list of numbers he had called. Indeed, Justice Stewart dissented specifically because he thought the difference was significant on the facts of that case. *See id.* at 747 ("such a list [of all the telephone numbers one called] easily could reveal ... the most intimate details of a person's life").

(ii). Application

The whole of one's movements over the course of a month is not constructively exposed to the public because, like a rap sheet, that whole reveals far more than the individual movements it comprises. The difference is not one of degree but of kind, for no single journey reveals the habits and patterns that mark the distinction between a day in the life

and a way of life, nor the departure from a routine that, like the dog that did not bark in the Sherlock Holmes story, may reveal even more.

As with the "mosaic theory" often invoked by the Government in cases involving national security information, "What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene." *CIA v. Sims*, 471 U.S. 159, 178 (1985) (internal quotation marks deleted); *see J. Roderick MacArthur Found. v. F.B.I.*, 102 F.3d 600, 604 (D.C. Cir. 1996). Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story.* A person who knows all of another's

---

* This case itself illustrates how the sequence of a person's movements may reveal more than the individual movements of which it is composed. Having tracked Jones's movements for a month, the Government used the resulting pattern — not just the location of a particular "stash house" or Jones's movements on any one trip or even day — as evidence of Jones's involvement in the cocaine trafficking business. The pattern the Government would document with the GPS data was central to its presentation of the case, as the prosecutor made clear in his opening statement:

> [T]he agents and investigators obtained an additional order and that was to install a GPS. ... They had to figure out where

travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups — and not just one such fact about a person, but all such facts.

Other courts have recognized prolonged surveillance of a person's movements may reveal an intimate picture of his life. *See Galella v. Onassis*, 353 F. Supp. 196, 227–28 (S.D.N.Y. 1972) ("Plaintiff's endless snooping constitutes tortious invasion of privacy .... [he] has insinuated himself into the very fabric of Mrs. Onassis' life") (*aff'd in relevant part* 487 F.2d 986, 994 & n.12 (2nd Cir. 1973) (if required to reach privacy issue "would be inclined to agree with" district court's treatment)). Indeed, they have reached that conclusion in cases involving prolonged GPS monitoring. *See People v. Weaver*, 909 N.E. 2d 1194, 1199 (N.Y. 2009) (Prolonged GPS monitoring "yields ... a highly detailed profile, not simply of where we go, but by easy inference, of our associations — political, religious, amicable and amorous, to name only a few — and of the pattern of our professional and avocational pursuits"); *State v. Jackson*, 76 P.3d 217, 224 (Wash. 2003) (en banc) ("In this age, vehicles are used to take people to a vast number of places that can reveal preferences, alignments, associations, personal ails and foibles. The GPS tracking devices record all of these travels, and thus can provide a detailed picture of one's life.").

---

is he going? When he says ten minutes, where is he going? Again, the pattern developed. ... And I want to ... just show you an example of how the pattern worked. ... The meetings are short. But you will again notice the pattern you will see in the coming weeks over and over again.

Tr. 11/15/07.

A reasonable person does not expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how long he stays there; rather, he expects each of those movements to remain "disconnected and anonymous," *Nader v. Gen. Motors Corp.*, 25 N.Y.2d 560, 572 (1970) (Breitel, J., concurring). In this way the extended recordation of a person's movements is, like the "manipulation of a bus passenger's carry-on" canvas bag in *Bond*, not what we expect anyone to do, and it reveals more than we expect anyone to know. 529 U.S. at 339.

logs of interest traffic ?

3. Was Jones's expectation of privacy reasonable?

It does not apodictically follow that, because the aggregation of Jones's movements over the course of a month was not exposed to the public, his expectation of privacy in those movements was reasonable; "legitimation of expectations of privacy must have a source outside the Fourth Amendment," such as "understandings that are recognized or permitted by society," *United States v. Jacobsen*, 466 U.S. 109, 123 n.22 (1984) (quoting *Rakas*, 439 U.S. at 143 n.12). So it is that, because the "Congress has decided ... to treat the interest in 'privately' possessing cocaine as illegitimate," "governmental conduct that can reveal whether a substance is cocaine, and no other arguably 'private' fact, compromises no legitimate privacy interest." *Id.* at 123.

The Government suggests Jones's expectation of privacy in his movements was unreasonable because those movements took place in his vehicle, on a public way, rather than inside his home. That the police tracked Jones's movements in his Jeep rather than in his home is certainly relevant to the reasonableness of his expectation of privacy; "in the sanctity of the home," the Court has observed, "*all*

details are intimate details," *Kyllo*, 533 U.S. at 37. A person does not leave his privacy behind when he walks out his front door, however. On the contrary, in *Katz* the Court clearly stated "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." 389 U.S. at 351. Or, as this court has said, outside the home, the "Fourth Amendment ... secur[es] for each individual a private enclave, a 'zone' bounded by the individual's own reasonable expectations of privacy." *Reporters Comm. for Freedom of Press v. AT&T*, 593 F.2d 1030, 1042–43 (1978).

Seems an inconsistency

Application of the test in *Katz* and its sequellae to the facts of this case can lead to only one conclusion: Society recognizes Jones's expectation of privacy in his movements over the course of a month as reasonable, and the use of the GPS device to monitor those movements defeated that reasonable expectation. As we have discussed, prolonged GPS monitoring reveals an intimate picture of the subject's life that he expects no one to have — short perhaps of his spouse. The intrusion such monitoring makes into the subject's private affairs stands in stark contrast to the relatively brief intrusion at issue in *Knotts*; indeed it exceeds the intrusions occasioned by every police practice the Supreme Court has deemed a search under *Katz*, such as a urine test, *see Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602 (1989) (urine test could "reveal a host of private medical facts about an employee, including whether he or she is epileptic, pregnant, or diabetic"); use of an electronic listening device to tap a payphone, *Katz*, 389 U.S. at 352 (user of telephone booth "entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world"); inspection of a traveler's luggage, *Bond*, 529 U.S. at 338 ("travelers are particularly concerned about their carry-on luggage"); or use of a thermal imaging device to discover the

temperature inside a home, *Kyllo*, 533 U.S. at 37 ("In the home, *all* details are intimate details"). very strong protection on home

We note without surprise, therefore, that the Legislature of California, in making it unlawful for anyone but a law enforcement agency to "use an electronic tracking device to determine the location or movement of a person," specifically declared "electronic tracking of a person's location without that person's knowledge violates that person's reasonable expectation of privacy," and implicitly but necessarily thereby required a warrant for police use of a GPS, California Penal Code section 637.7, Stats. 1998 c. 449 (S.B. 1667) § 2. Several other states have enacted legislation imposing civil and criminal penalties for the use of electronic tracking devices and expressly requiring exclusion of evidence produced by such a device unless obtained by the police acting pursuant to a warrant. *See, e.g.*, Utah Code Ann. §§ 77-23a-4, 77-23a-7, 77-23a-15.5; Minn Stat §§ 626A.37, 626A.35; Fla Stat §§ 934.06, 934.42; S.C. Code Ann § 17-30-140; Okla. Stat, tit 13, §§ 176.6, 177.6; Haw. Rev. Stat §§ 803-42, 803-44.7; 18 Pa. Cons. Stat § 5761.

Although perhaps not conclusive evidence of nationwide "societal understandings," *Jacobsen*, 466 U.S. at 123 n.22, these state laws are indicative that prolonged GPS monitoring defeats an expectation of privacy that our society recognizes as reasonable. So, too, are the considered judgments of every court to which the issue has been squarely presented. *See Weaver*, 12 N.Y.3d at 447 ("the installation and use of a GPS device to monitor an individual's whereabouts requires a warrant supported by probable cause"); *Jackson*, 76 P.3d at 223-24 (under art. I, § 7 of Washington State Constitution, which "focuses on those privacy interests which citizens of this state have held, and should be entitled to hold, safe from governmental trespass," "use of a GPS device on a private

vehicle involves a search and seizure"); *cf. Commonwealth v. Connolly*, 913 N.E.2d 356, 369–70 (Ma. 2009) (installation held a seizure). The federal circuits that have held use of a GPS device is not a search were not alert to the distinction drawn in *Knotts* between short-term and prolonged surveillance,* but we have already explained our disagreement on that collateral point.

4. Visual surveillance distinguished

The Government would have us abjure this conclusion on the ground that "[Jones's] argument logically would prohibit even visual surveillance of persons or vehicles located in public places and exposed to public view, which clearly is not the law." We have already explained why Jones's argument does not "logically ... prohibit" much visual surveillance: Surveillance that reveals only what is already exposed to the

---

* One federal district court and two state courts have also held use of a GPS device is not *per se* a search, but none was presented with the argument that prolonged use of a GPS device to track an individual's movements is meaningfully different from short-term surveillance. *See United States v. Moran*, 349 F. Supp. 2d 425, 467–68 (N.D.N.Y. 2005) (police used GPS device to track defendant during one-day drive from Arizona to New York); *State v. Sveum*, 269 N.W.2d 53, 59 (Wis. Ct. App. 2009) ("Sveum implicitly concedes that ... using [a GPS device] to monitor *public* travel does not implicate the Fourth Amendment. He contends, however, that because the GPS device permitted the police to monitor the location of his car while it was in his garage ... all of the information obtained from the GPS device should have been suppressed."); *Stone v. State*, 941 A.2d 1238 (Md. 2008) (holding, in light of *Knotts*, that lower court "did not abuse its discretion in cutting short testimony" about use of GPS device; appellant did not cite *Knotts* in his briefs or affirmatively argue use of device was a search).

public — such as a person's movements during a single journey — is not a search. *See Knotts*, 460 U.S. at 285.

Regarding visual surveillance so prolonged it reveals information not exposed to the public, we note preliminarily that the Government points to not a single actual example of visual surveillance that will be affected by our holding the use of the GPS in this case was a search. No doubt the reason is that practical considerations prevent visual surveillance from lasting very long.* Continuous human surveillance for a week would require all the time and expense of several police officers, while comparable photographic surveillance would require a net of video cameras so dense and so widespread as to catch a person's every movement, plus the manpower to piece the photographs together. Of course, as this case and some of the GPS cases in other courts illustrate, *e.g.*, *Weaver*, 12 N.Y.3d at 447, 459 (holding use of GPS device to track suspect for 65 days was search); *Jackson*, 76 P.3d 261–62 (holding use of GPS device to track suspect for two and one-half weeks was search), prolonged GPS monitoring is not similarly constrained. On the contrary, the marginal cost of an additional day — or week, or month — of GPS monitoring is effectively zero. Nor, apparently, is the fixed cost of installing a GPS device significant; the Los Angeles Police

---

* According to the former Chief of the LAPD, keeping a suspect under "constant and close surveillance" is "not only more costly than any police department can afford, but in the vast majority of cases it is impossible." W.H. Parker, *Surveillance by Wiretap or Dictograph: Threat or Protection?*, 42 Cal. L. Rev. 727, 734 (1954). Or as one of the Special Agents involved in the investigation of Jones testified at trial: "Physical surveillance is actually hard, you know. There's always chances of getting spotted, you know, the same vehicle always around, so we decided to use GPS technology." Tr. 11/21/07 at 114.

Department can now affix a GPS device to a passing car simply by launching a GPS-enabled dart.* For these practical reasons, and not by virtue of its sophistication or novelty, the advent of GPS technology has occasioned a heretofore unknown type of intrusion into an ordinarily and hitherto private enclave.

The Government's argument — that our holding the use of the GPS device was a search necessarily implicates prolonged visual surveillance — fails even on its own terms. That argument relies implicitly upon an assumption rejected explicitly in *Kyllo*, to wit, that the means used to uncover private information play no role in determining whether a police action frustrates a person's reasonable expectation of privacy; when it comes to the Fourth Amendment, means do matter. *See* 533 U.S. at 35 n.2 ("The fact that equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment"). For example, the police may without a warrant record one's conversations by planting an undercover agent in one's midst, *Lopez v. United States*, 373 U.S. 427, 429 (1963), but may not do the same by wiretapping one's phone, even "without any trespass," *Katz*, 389 U.S. 347, 353 (1967). Quite simply, in the former case one's reasonable

* "The darts consist of a miniaturized GPS receiver, radio transmitter, and battery embedded in a sticky compound material. When fired at a vehicle, the compound adheres to the target, and thereafter permits remote real-time tracking of the target from police headquarters." Renee McDonald Hutchins, *Tied Up in Knotts? GPS Technology and the Fourth Amendment*, 55 UCLA L. Rev. 409, 419 (2007); *see also* Richard Winton, *LAPD Pursues High-Tech End to High-Speed Chases*, L.A. Times, Feb. 3, 2006, at B1. GPS darts are used in exigent circumstances and for only as long as it takes to interdict the subject driver without having to engage in a high-speed chase on a public way.

expectation of control over one's personal information would not be defeated; in the latter it would be. See *Reporters Committee*, 489 U.S. at 763 ("both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person").

This case does not require us to, and therefore we do not, decide whether a hypothetical instance of prolonged visual surveillance would be a search subject to the warrant requirement of the Fourth Amendment. As the Supreme Court said in *Dow Chemical Co. v. United States*, "Fourth Amendment cases must be decided on the facts of each case, not by extravagant generalizations. 'We have never held that potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment.'" 476 U.S. 227, 238 n.5 (1986) (quoting *United States v. Karo*, 468 U.S. 705, 712 (1984)); *see also City of Ontario v. Quon*, 130 S. Ct. 2619, 2629 (2010) ("Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations"). By the same token, we refuse to hold this "search is not a search," *Kyllo*, 533 U.S. at 32, merely because a contrary holding might at first blush seem to implicate a different but intuitively permissible practice. *See Nat'l Fed'n of Fed. Employees v. Weinberger*, 818 F.2d 935, 942 (D.C. Cir. 1987) ("Few legal issues in the Fourth Amendment domain are so pure that they do not turn on *any* facts or circumstances peculiar to the case"). Instead, just as the Supreme Court in *Knotts* reserved the lawfulness of prolonged beeper surveillance, we reserve the lawfulness of prolonged visual surveillance.

B. Was the Search Reasonable Nonetheless?

A search conducted without a warrant is "per se unreasonable under the Fourth Amendment — subject only to a few specifically established and well-delineated exceptions." *Katz*, 389 U.S. at 357. Here, because the police installed the GPS device on Jones's vehicle without a valid warrant,* the Government argues the resulting search can be upheld as a reasonable application of the automobile exception to the warrant requirement. Under that exception, "[i]f a car is readily mobile and probable cause exists to believe it contains contraband, the Fourth Amendment ... permits police to search the vehicle without more." *Pennsylvania v. Labron*, 518 U.S. 938, 940 (1996).

As Jones points out, this argument is doubly off the mark. First, the Government did not raise it below. *See Bryant v. Gates*, 532 F.3d 888, 898 (D.C. Cir. 2008) (argument not made in district court is forfeited). Second, the automobile exception permits the police to search a car without a warrant if they have reason to believe it contains contraband; the exception does not authorize them to install a tracking device on a car without the approval of a neutral magistrate. *See Delaware v. Prouse*, 440 U.S. 648, 662–63 (1979) ("Were the individual subject to unfettered governmental intrusion every time he entered his automobile, the security guaranteed by the Fourth Amendment would be seriously circumscribed").

---

* The police had obtained a warrant to install the GPS device in D.C. only, but it had expired before they installed it — which they did in Maryland. When challenged in the district court, the Government "conceded ... the violations" of the court's order, "confine[d] its arguments to the issue of whether or not a court order was required[,] and assert[ed] that it was not." Government's Omnibus Response to Defendant's Legal Motions.

C. Was the Error Harmless?

Finally, the Government argues in a terse and conclusory few lines that the district court's error in admitting evidence obtained by use of the GPS device was harmless. "The beneficiary of a constitutional error [must prove] beyond a reasonable doubt that the error complained of did not contribute to the verdict obtained." *Chapman v. California*, 386 U.S. 18, 24 (1967).

According to the Government, "Overwhelming evidence implicated [Jones] in the drug-distribution conspiracy." Overwhelming evidence certainly showed there was a conspiracy to distribute and to possess with intent to distribute drugs based out of 9508 Potomac Drive, Ft. Washington, Maryland, where police found $850,000 in cash, 97 kilograms of cocaine, and one kilogram of cocaine base. The evidence linking Jones to that conspiracy, however, was not strong, let alone overwhelming.

The Government points to no evidence of a drug transaction in which Jones was involved, nor any evidence that Jones ever possessed any drugs. Instead it relies upon (1) the testimony of admitted participants in the conspiracy, one of whom (Bermea) was at the Potomac Drive house when the police arrived — to the effect that Jones was the ringleader of the operation and frequented the Potomac Drive house, (2) data showing Jones used his cell-phone frequently and often called some of the conspirators, including one whose phone was found at the Potomac Drive house, (3) leases in Jones's name for other properties the Government alleged were used in furtherance of the conspiracy, (4) currency seized from Jones's Jeep and mini-van, and (5) physical and photographic surveillance showing Jones visited the Potomac Drive house a few times. Jones's defense responded to each type of

evidence as follows: (1) the cooperating witnesses had cut deals with the Government and were not credible, (2) the cell-phone records and (5) visits to Potomac Drive showed only that Jones knew the participants in the conspiracy, (3) Jones leased the other properties for legitimate purposes and no drugs were found there, (4) and his nightclub was a cash business.

The GPS data were essential to the Government's case. By combining them with Jones's cell-phone records the Government was able to paint a picture of Jones's movements that made credible the allegation that he was involved in drug trafficking. In his closing statement the Government attorney summarized this way the inference he was asking the jury to draw:

> [W]hen there is a conversation with Bermea and [Jones] says, I'm coming to see you, or I'll be there in ten minutes, and within a while ... the GPS shows that that vehicle is in Potomac Drive, how does that all fit together? Well it fits together exactly as you know. That the defendant is going to 9508 Potomac Drive, and there's no reason anyone goes there other than drug activity.
>
> ....
>
> Then, that follows these series of conversations, day after day, GPS reading after GPS reading, with the defendant speaking with [Bermea] and then the vehicle coming to Potomac Drive. ... You'll have the timeline. You've got the conversations. I won't go through them all."

Tr. 1/3/08 at 114–18. As mentioned earlier, the Government had also stressed in its opening remarks, which would color

the jury's understanding of the whole case, that the GPS data would demonstrate Jones's involvement in the conspiracy.

To be sure, absent the GPS data a jury reasonably might have inferred Jones was involved in the conspiracy. "We are not concerned here," however, "with whether there was sufficient evidence on which [Jones] could have been convicted without the evidence complained of"; rather our concern is with "whether there is a reasonable possibility that the evidence complained of might have contributed to the conviction." *Fahy v. Connecticut*, 375 U.S. 85, 86–87 (1963). Without the GPS data the evidence that Jones was actually involved in the conspiracy is so far from "overwhelming" that we are constrained to hold the Government has not carried its burden of showing the error was harmless beyond a reasonable doubt.

IV. Conclusion

Maynard's conviction and sentence are affirmed because neither any of the appellants' joint arguments nor Maynard's individual argument warrants reversal. Jones's conviction is reversed because it was obtained with evidence procured in violation of the Fourth Amendment.

So ordered.

U.S. Supreme Court

UNITED STATES v. MILLER, 425 U.S. 435 (1976)

425 U.S. 435

UNITED STATES v. MILLER.
CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FIFTH CIRCUIT.

No. 74-1179.

Argued January 12, 1976.
Decided April 21, 1976.

Read 10/18

Respondent, who had been charged with various federal offenses, made a pretrial motion to suppress microfilms of checks, deposit slips, and other records relating to his accounts at two banks, which maintained the records pursuant to the Bank Secrecy Act of 1970 (Act). He contended that the subpoenas duces tecum pursuant to which the material had been produced by the banks were defective and that the records had thus been illegally seized in violation of the Fourth Amendment. Following denial of his motion, respondent was tried and convicted. The Court of Appeals reversed, having concluded that the subpoenaed documents fell within a constitutionally protected zone of privacy. Held: Respondent possessed no Fourth Amendment interest in the bank records that could be vindicated by a challenge to the subpoenas, and the District Court therefore did not err in denying the motion to suppress. Pp. 440-446.

(a) The subpoenaed materials were business records of the banks, not respondent's private papers. Pp. 440-441.

(b) There is no legitimate "expectation of privacy" in the contents of the original checks and deposit slips, since the checks are not confidential communications but negotiable instruments to be used in commercial transactions, and all the documents obtained contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business. The Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities. The Act's recordkeeping requirements do not alter these considerations so as to create a protectable Fourth Amendment interest of a bank depositor in the bank's records of his account. Pp. 441-443.

(c) Issuance of a subpoena to a third party does not violate a defendant's rights, even if a criminal prosecution is contemplated at the time the subpoena is issued. California Bankers Assn. v. Shultz, 416 U.S. 21, 53 . Pp. 444-445. [425 U.S. 435, 436]

(d) Access to bank records under the Act is to be controlled by "existing legal process." That does not mean that greater judicial scrutiny, equivalent to that required for a search warrant, is necessary when a subpoena is used to obtain a depositor's bank records. Pp. 445-446.

500 F.2d 751, reversed and remanded.

POWELL, J., delivered the opinion of the Court, in which BURGER, C. J., and STEWART, WHITE, BLACKMUN, REHNQUIST, and STEVENS, JJ., joined. BRENNAN, J., post, p. 447, and MARSHALL, J., post, p. 455, filed dissenting opinions.

Deputy Solicitor General Wallace argued the cause for the United States. With him on the brief were Solicitor General Bork, Assistant Attorney General Thornburgh, Sidney M. Glazer, and Ivan Michael Schaeffer.

D. L. Rampey, Jr., by appointment of the Court, 422 U.S. 1054 , argued the cause and filed a brief for respondent.

MR. JUSTICE POWELL delivered the opinion of the Court.

Respondent was convicted of possessing an unregistered still, carrying on the business of a distiller without giving bond and with intent to defraud the Government of whiskey tax, possessing 175 gallons of whiskey upon which no taxes had been paid, and conspiring to defraud the United States of tax revenues. 26 U.S.C. 5179, 5205, 5601 et seq.; 18 U.S.C. 371. Prior to trial respondent moved to suppress copies of checks and other bank records obtained by means of allegedly defective subpoenas duces tecum served upon two banks at which he had accounts. The records had been maintained by the banks in compliance with the requirements of the Bank Secrecy Act of 1970, 84 Stat. 1114, 12 U.S.C. 1829b (d). [425 U.S. 435, 437]

The District Court overruled respondent's motion to suppress, and the evidence was admitted. The Court of Appeals for the Fifth Circuit reversed on the ground that a depositor's Fourth Amendment rights are violated when bank records maintained pursuant to the Bank Secrecy Act are obtained by means of a defective subpoena. It held that any evidence so obtained must be suppressed. Since we find that respondent had no protectable Fourth Amendment interest in the subpoenaed documents, we reverse the decision below.

I

On December 18, 1972, in response to an informant's tip, a deputy sheriff from Houston County, Ga., stopped a van-type truck occupied by two of respondent's alleged co-conspirators. The truck contained distillery apparatus and raw material. On January 9, 1973, a fire broke out in a Kathleen, Ga., warehouse rented to respondent. During the blaze firemen and sheriff department officials discovered a 7,500-gallon-capacity distillery, 175 gallons of non-tax-paid whiskey, and related paraphernalia.

Two weeks later agents from the Treasury Department's Alcohol, Tobacco and Firearms Bureau presented grand jury subpoenas issued in blank by the clerk of the District Court, and completed by the United States Attorney's office, to the presidents of the Citizens & Southern National Bank of Warner Robins and the Bank of Byron, where respondent maintained accounts. The subpoenas required the two presidents to appear on January 24, 1973, and to produce

> "all records of accounts, i. e., savings, checking, loan or otherwise, in the name of Mr. Mitch Miller [respondent], 3859 Mathis Street, Macon, Ga. and/or Mitch Miller Associates, 100 Executive [425 U.S. 435, 438] Terrace, Warner Robins, Ga., from October 1, 1972, through the present date [January 22, 1973, in the case of the Bank of Byron, and January 23, 1973, in the

case of the Citizens & Southern National Bank of Warner Robins]."

The banks did not advise respondent that the subpoenas had been served but ordered their employees to make the records available and to provide copies of any documents the agents desired. At the Bank of Byron, an agent was shown microfilm records of the relevant account and provided with copies of one deposit slip and one or two checks. At the Citizens & Southern National Bank microfilm records also were shown to the agent, and he was given copies of the records of respondent's account during the applicable period. These included all checks, deposit slips, two financial statements, and three monthly statements. The bank presidents were then told that it would not be necessary to appear in person before the grand jury.

The grand jury met on February 12, 1973, 19 days after the return date on the subpoenas. Respondent and four others were indicted. The overt acts alleged to have been committed in furtherance of the conspiracy included three financial transactions - the rental by respondent of the van-type truck, the purchase by respondent of radio equipment, and the purchase by respondent of a quantity of sheet metal and metal pipe. The record does not indicate whether any of the bank records were in fact presented to the grand jury. They were used in the investigation and provided "one or two" investigatory leads. Copies of the checks also were introduced at trial to establish the overt acts described above.

In his motion to suppress, denied by the District Court, respondent contended that the bank documents were illegally seized. It was urged that the subpoenas were [425 U.S. 435, 439] defective because they were issued by the United States Attorney rather than a court, no return was made to a court, and the subpoenas were returnable on a date when the grand jury was not in session. The Court of Appeals reversed. 500 F.2d 751 (1974). Citing the prohibition in Boyd v. United States, 116 U.S. 616, 622 (1886), against "compulsory production of a man's private papers to establish a criminal charge against him," the court held that the Government had improperly circumvented Boyd's protections of respondent's Fourth Amendment right against "unreasonable searches and seizures" by "first requiring a third party bank to copy all of its depositors' personal checks and then, with an improper invocation of legal process, calling upon the bank to allow inspection and reproduction of those copies." 500 F.2d, at 757. The court acknowledged that the recordkeeping requirements of the Bank Secrecy Act had been held to be constitutional on their face in California Bankers Assn. v. Shultz, 416 U.S. 21 (1974), but noted that access to the records was to be controlled by "existing legal process." See id., at 52. The subpoenas issued here were found not to constitute adequate "legal process." The fact that the bank officers cooperated voluntarily was found to be irrelevant, for "he whose rights are threatened by the improper disclosure here was a bank depositor, not a bank official." 500 F.2d, at 758.

The Government contends that the Court of Appeals erred in three respects: (i) in finding that respondent had the Fourth Amendment interest necessary to entitle him to challenge the validity of the subpoenas duces tecum through his motion to suppress; (ii) in holding that the subpoenas were defective; and (iii) in determining that suppression of the evidence obtained was the appropriate remedy if a constitutional violation did take place. [425 U.S. 435, 440]

We find that there was no intrusion into any area in which respondent had a protected Fourth Amendment interest and that the District Court therefore correctly denied respondent's motion to suppress. Because we reverse the decision of the Court of Appeals on that ground alone, we do not reach the Government's latter two contentions.

II

In Hoffa v. United States, 385 U.S. 293, 301 -302 (1966), the Court said that "no interest legitimately protected by the Fourth Amendment" is implicated by governmental investigative activities unless there is an intrusion into a zone of privacy, into "the security a man relies upon when he places himself or his property within a constitutionally protected area." The Court of Appeals, as noted above, assumed that respondent had the necessary Fourth Amendment interest, pointing to the language in Boyd v. United States, supra, at 622, which describes that Amendment's protection against the "compulsory production of a man's private papers." 1 We think that the Court of Appeals erred in finding the subpoenaed documents to fall within a protected zone of privacy.

On their face, the documents subpoenaed here are not respondent's "private papers." Unlike the claimant in Boyd, respondent can assert neither ownership nor possession. Instead, these are the business records of the banks. As we said in California Bankers Assn. v. Shultz, supra, at 48-49, "[b]anks are . . . not . . . neutrals in transactions involving negotiable instruments, but parties to the instruments with a substantial stake in their continued availability and acceptance." The records of respondent's [425 U.S. 435, 441] accounts, like "all of the records [which are required to be kept pursuant to the Bank Secrecy Act,] pertain to transactions to which the bank was itself a party." Id., at 52.

Respondent argues, however, that the Bank Secrecy Act introduces a factor that makes the subpoena in this case the functional equivalent of a search and seizure of the depositor's "private papers." We have held, in California Bankers Assn. v. Shultz, supra, at 54, that the mere maintenance of records pursuant to the requirements of the Act "invade[s] no Fourth Amendment right of any depositor." But respondent contends that the combination of the recordkeeping requirements of the Act and the issuance of a subpoena 2 to obtain those records permits the Government to circumvent the requirements of the Fourth Amendment by allowing it to obtain a depositor's private records without complying with the legal requirements that would be applicable had it proceeded against him directly. 3 Therefore, we must address the question whether the compulsion embodied in the Bank Secrecy Act as exercised in this case creates a Fourth Amendment interest in the depositor where none existed before. This question was expressly reserved [425 U.S. 435, 442] in California Bankers Assn., supra, at 53-54, and n. 24.

Respondent urges that he has a Fourth Amendment interest in the records kept by the banks because they are merely copies of personal records that were made available to the banks for a limited purpose and in which he has a reasonable expectation of privacy. He relies on this Court's statement in Katz v. United States, 389 U.S. 347, 353 (1967), quoting Warden v. Hayden, 387 U.S. 294, 304 (1967), that "we have . . . departed from the narrow view" that "`property interests control the right of the Government to search and seize,'" and that a "search and seizure" become unreasonable when the Government's activities violate "the privacy upon which [a person] justifiably relie[s]." But in Katz the Court also stressed that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection." 389 U.S., at 351 . We must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate "expectation of privacy" concerning their contents. Cf. Couch v. United States. 400 U.S. 322, 335 (1973).

Even if we direct our attention to the original checks and deposit slips, rather than to the microfilm copies actually viewed and obtained by means of the subpoena, we perceive no legitimate "expectation of privacy" in their contents. The checks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business. The lack of any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress in enacting the Bank

Secrecy Act, the expressed purpose of which is to require records [425 U.S. 435, 443] to be maintained because they "have a high degree of usefulness in criminal, tax, and regulatory investigations and proceedings." 12 U.S.C. 1829b (a) (1). Cf. Couch v. United States, supra, at 335.

The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. United States v. White, 401 U.S. 745, 751 -752 (1971). 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 752; Hoffa v. United States, 385 U.S., at 302 ; Lopez v. United States, 373 U.S. 427 (1963). 4

This analysis is not changed by the mandate of the Bank Secrecy Act that records of depositors' transactions be maintained by banks. In California Bankers Assn. v. Shultz, 416 U.S., at 52 -53, we rejected the contention that banks, when keeping records of their depositors' transactions pursuant to the Act, are acting solely as agents of the Government. But, even if the banks could be said to have been acting solely as Government agents in transcribing the necessary information and complying without protest 5 with the requirements of the subpoenas, there would be no intrusion upon the depositors' Fourth Amendment rights. See Osborn v. United States, 385 U.S. 323 (1966); Lewis v. United States, 385 U.S. 206 (1966). [425 U.S. 435, 444]

III

Since no Fourth Amendment interests of the depositor are implicated here, this case is governed by the general rule that the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant, even if a criminal prosecution is contemplated at the time the subpoena is issued. California Bankers Assn. v. Shultz, supra, at 53; Donaldson v. United States, 400 U.S. 517, 537 (1971) (Douglas, J., concurring). Under these principles, it was firmly settled, before the passage of the Bank Secrecy Act, that an Internal Revenue Service summons directed to a third-party bank does not violate the Fourth Amendment rights of a depositor under investigation. See First National Bank of Mobile v. United States, 267 U.S. 576 (1925), aff'g 295 F. 142 (SD Ala. 1924). See also California Bankers Assn. v. Shultz, supra, at 53; Donaldson v. United States, supra, at 522.

Many banks traditionally kept permanent records of their depositors' accounts, although not all banks did so and the practice was declining in recent years. By requiring that such records be kept by all banks, the Bank Secrecy Act is not a novel means designed to circumvent established Fourth Amendment rights. It is merely an attempt to facilitate the use of a proper and longstanding law enforcement technique by insuring that records are available when they are needed. 6 [425 U.S. 435, 445]

We hold that the District Court correctly denied respondent's motion to suppress, since he possessed no Fourth Amendment interest that could be vindicated by a challenge to the subpoenas.

IV

Respondent contends not only that the subpoenas duces tecum directed against the banks infringed his Fourth Amendment rights, but that a subpoena issued to a bank to obtain records maintained pursuant to the Act is subject to more stringent Fourth Amendment requirements than is the ordinary subpoena. In making this assertion he relies on our statement in California Bankers Assn., supra, at 52, that access to the records maintained by banks under the Act is to be controlled by "existing legal process." 7

In Oklahoma Press Pub. Co. v. Walling, 327 U.S. 186, 208 (1946), the Court said that "the Fourth [Amendment], if applicable [to subpoenas for the production of business records and papers], at the most guards against abuse only by way of too much indefiniteness or breadth in the things required to be `particularly described,' if also the inquiry is one the demanding [425 U.S. 435, 446] agency is authorized by law to make and the materials specified are relevant." See also United States v. Dionisio, 410 U.S. 1, 11 -12 (1973). Respondent, citing United States v. United States District Court, 407 U.S. 297 (1972), in which we discussed the application of the warrant requirements of the Fourth Amendment to domestic security surveillance through electronic eavesdropping, suggests that greater judicial scrutiny, equivalent to that required for a search warrant, is necessary when a subpoena is to be used to obtain bank records of a depositor's account. But in California Bankers Assn., 416 U.S., at 52 , we emphasized only that access to the records was to be in accordance with "existing legal process." There was no indication that a new rule was to be devised, or that the traditional distinction between a search warrant and a subpoena would not be recognized. 8

In any event, for the reasons stated above, we hold that respondent lacks the requisite Fourth Amendment interest to challenge the validity of the subpoenas. 9

V

The judgment of the Court of Appeals is reversed. The court deferred decision on whether the trial court had improperly overruled respondent's motion to suppress [425 U.S. 435, 447] distillery apparatus and raw material seized from a rented truck. We remand for disposition of that issue.

So ordered.

Footnotes

[Footnote 1] The Fourth Amendment implications of Boyd as it applies to subpoenas duces tecum have been undercut by more recent cases. Fisher v. United States, ante, at 407-409. See infra, at 445-446.

[Footnote 2] Respondent appears to contend that a depositor's Fourth Amendment interest comes into play only when a defective subpoena is used to obtain records kept pursuant to the Act. We see no reason why the existence of a Fourth Amendment interest turns on whether the subpoena is defective. Therefore, we do not limit our consideration to the situation in which there is an alleged defect in the subpoena served on the bank.

[Footnote 3] It is not clear whether respondent refers to attempts to obtain private documents through a subpoena issued directly to the depositor or through a search pursuant to a warrant. The question whether personal business records may be seized pursuant to a valid warrant is before this Court in No. 74-1646, Andresen v. Maryland, cert. granted, 423 U.S. 822 .

[Footnote 4] We do not address here the question of evidentiary privileges, such as that protecting communications between an attorney and his client. Cf. Fisher v. United States, ante, at 403-405.

[Footnote 5] Nor did the banks notify respondent, a neglect without legal consequences here, however unattractive it may be.

[Footnote 6] Respondent does not contend that the subpoenas infringed upon his First Amendment

rights. There was no blanket reporting requirement of the sort we addressed in Buckley v. Valeo, 424 U.S. 1, 60 -84 (1976), nor any allegation of an improper inquiry into protected associational activities of the sort presented in Eastland v. United States Servicemen's Fund, 421 U.S. 491 (1975).

We are not confronted with a situation in which the Government, through "unreviewed executive discretion," has made a wide-ranging [425 U.S. 435, 445] inquiry that unnecessarily "touch[es] upon intimate areas of an individual's personal affairs." California Bankers Assn. v. Shultz, 416 U.S., at 78 -79 (POWELL, J., concurring). Here the Government has exercised its powers through narrowly directed subpoenas duces tecum subject to the legal restraints attendant to such process. See Part IV, infra.

[Footnote 7] This case differs from Burrows v. Superior Court, 13 Cal. 3d 238, 529 P.2d 590 (1974), relied on by MR. JUSTICE BRENNAN in dissent, in that the bank records of respondent's accounts were furnished in response to "compulsion by legal process" in the form of subpoenas duces tecum. The court in Burrows found it "significant . . . that the bank [in that case] provided the statements to the police in response to an informal oral request for information." Id., at 243, 529 P.2d, at 593.

[Footnote 8] A subpoena duces tecum issued to obtain records is subject to no more stringent Fourth Amendment requirements than is the ordinary subpoena. A search warrant, in contrast, is issuable only pursuant to prior judicial approval and authorizes Government officers to seize evidence without requiring enforcement through the courts. See United States v. Dionisio, 410 U.S. 1, 9 -10 (1973).

[Footnote 9] There is no occasion for us to address whether the subpoenas complied with the requirements outlined in Oklahoma Press Pub. Co. v. Walling, 327 U.S. 186 (1946). The banks upon which they were served did not contest their validity.

MR. JUSTICE BRENNAN, dissenting.

The pertinent phrasing of the Fourth Amendment - "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated" - is virtually in haec verba as Art. I, 19, of the California Constitution - "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable seizures and searches, shall not be violated." The California Supreme Court has reached a conclusion under Art. I, 19, in the same factual situation, contrary to that reached by the Court today under the Fourth Amendment. 1 I dissent because in my view the California Supreme Court correctly interpreted the relevant constitutional language.

In Burrows v. Superior Court, 13 Cal. 3d 238, 529 P.2d 590 (1974), the question was whether bank statements or copies thereof relating to an accused's bank accounts obtained by the sheriff and prosecutor without [425 U.S. 435, 448] benefit of legal process, 2 but with the consent of the bank, were acquired as a result of an illegal search and seizure. The California Supreme Court held that the accused had a reasonable expectation of privacy in his bank statements and records, that the voluntary relinquishment of such records by the bank at the request of the sheriff and prosecutor did not constitute a valid consent by the accused, and that the acquisition by the officers of the records therefore was the result of an illegal search and seizure. In my view the same conclusion, for the reasons stated by the California Supreme Court, is compelled in this case under the practically identical phrasing of the Fourth Amendment. Addressing the threshold question whether the accused's right of privacy was invaded, and relying in part on the decision of the Court of Appeals in this case, Mr. Justice Mosk stated in his excellent opinion for a unanimous court:

"It cannot be gainsaid that the customer of a bank expects that the documents, such as checks, which he transmits to the bank in the course of his business operations, will remain private, and that such an expectation is reasonable. The prosecution concedes as much, although it asserts that this expectation [425 U.S. 435, 449] is not constitutionally cognizable. Representatives of several banks testified at the suppression hearing that information in their possession regarding a customer's account is deemed by them to be confidential.

"In the present case, although the record establishes that copies of petitioner's bank statements rather than of his checks were provided to the officer, the distinction is not significant with relation to petitioner's expectation of privacy. That the bank alters the form in which it records the information transmitted to it by the depositor to show the receipt and disbursement of money on a bank statement does not diminish the depositor's anticipation of privacy in the matters which he confides to the bank. A bank customer's reasonable expectation is that, absent compulsion by legal process, the matters he reveals to the bank will be utilized by the bank only for internal banking purposes. Thus, we hold petitioner had a reasonable expectation that the bank would maintain the confidentiality of those papers which originated with him in check form and of the bank statements into which a record of those same checks had been transformed pursuant to internal bank practice.

. . . . .

"The People assert that no illegal search and seizure occurred here because the bank voluntarily provided the statements to the police, and the bank rather than the police conducted the search of its records for papers relating to petitioner's accounts. If, as we conclude above, petitioner has a reasonable expectation of privacy in the bank statements, the voluntary relinquishment of such records by the bank at the request of the police does not constitute [425 U.S. 435, 450] a valid consent by this petitioner. . . . It is not the right of privacy of the bank but of the petitioner which is at issue, and thus it would be untenable to conclude that the bank, a neutral entity with no significant interest in the matter, may validly consent to an invasion of its depositors' rights. However, if the bank is not neutral, as for example where it is itself a victim of the defendant's suspected wrongdoing, the depositor's right of privacy will not prevail.

"Our rationale is consistent with the recent decision of United States v. Miller (5th Cir. 1974) 500 F.2d 751. In Miller, the United States Attorney, without the defendant's knowledge, issued subpoenas to two banks in which the defendant maintained accounts, ordering the production of `all records of accounts' in the name of the defendant. The banks voluntarily provided the government with copies of the defendant's checks and a deposit slip; these items were introduced into evidence at the trial which led to his conviction. The circuit court reversed the conviction. It held that the defendant's rights under the Fourth Amendment were violated by the search because the subpoena was issued by the United States Attorney rather than by a court or grand jury, and the bank's voluntary compliance with the subpoena was irrelevant since it was the depositor's right to privacy which was threatened by the disclosure.

"We hold that any bank statements or copies thereof obtained by the sheriff and prosecutor without the benefit of legal process were acquired as the result of an illegal search and seizure (Cal. Const., art. I, 13), and that the trial court should have granted the motion to suppress such documents.

. . . . . [425 U.S. 435, 451]

"The underlying dilemma in this and related cases is that the bank, a detached and disinterested entity, relinquished the records voluntarily. But that circumstance should not be crucial. For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account. In the course of such dealings, a depositor reveals many aspects of his personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography. While we are concerned in the present case only with bank statements, the logical extension of the contention that the bank's ownership of records permits free access to them by any police officer extends far beyond such statements to checks, savings, bonds, loan applications, loan guarantees, and all papers which the customer has supplied to the bank to facilitate the conduct of his financial affairs upon the reasonable assumption that the information would remain confidential. To permit a police officer access to these records merely upon his request, without any judicial control as to relevancy or other traditional requirements of legal process, and to allow the evidence to be used in any subsequent criminal prosecution against a defendant, opens the door to a vast and unlimited range of very real abuses of police power.

"Cases are legion that condemn violent searches and invasions of an individual's right to the privacy of his dwelling. The imposition upon privacy, although perhaps not so dramatic, may be equally devastating when other methods are employed. Development of photocopying machines, electronic computers and other sophisticated instruments have [425 U.S. 435, 452] accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds. Consequently judicial interpretations of the reach of the constitutional protection of individual privacy must keep pace with the perils created by these new devices." 13 Cal. 3d, at 243-248, 529 P.2d, at 593-596 (footnote omitted).

The California Supreme Court also addressed the question of the relevance of California Bankers Assn. v. Shultz, 416 U.S. 21 (1974). In my view, for the reasons stated in Burrows, the decision of the Court of Appeals under review today, is in no way inconsistent with California Bankers. 3 The California Supreme Court said:

"[California Bankers] held, in a six-three decision, that the bank's rights under the Fourth Amendment were not abridged by the regulation, and that the depositor plaintiffs lacked standing to challenge the reporting requirement because there was no showing that they engaged in the type of transaction to which the regulation referred.

"The concurring views of two justices who provided the necessary votes to create a majority are of particular interest. Justice Powell's opinion, joined by Justice Blackmun [416 U.S., at 78] makes clear that a significant extension of the reporting requirement would pose substantial constitutional questions, and that concurrence with the [425 U.S. 435, 453] majority was based upon the provisions of the act as narrowed by the regulations. He wrote, `In their full reach, the reports apparently authorized by the open-ended language of the Act touch upon intimate areas of an individual's personal affairs. Financial transactions can reveal much about a person's activities, associations, and beliefs. At some point, governmental intrusion upon these areas would implicate legitimate expectations of privacy. Moreover, the potential for abuse is particularly acute where, as here, the legislative scheme permits access to this information without invocation of the judicial process. In such instances, the important responsibility for balancing societal and individual interests is left to unreviewed executive discretion, rather than the scrutiny of a neutral magistrate. United States v. United States District Court, 407 U.S. 297,

316 -317.' [416 U.S., at 78 -79.]

"Justices Douglas and Marshall dissented on the ground that the act violated the Fourth Amendment. Justice Brennan also filed a dissent, stating that the recordkeeping and reporting requirements of the act constituted an impermissibly broad grant of power to the Secretary.

". . . [T]he only federal case decided after Shultz and directly confronting the issue of the depositor's rights is entirely consistent with the views we have set forth above. . . . Miller holds that Shultz may not be interpreted as `proclaiming open season on personal bank records' or as permitting the government to circumvent the Fourth Amendment by first requiring banks to copy their depositors' checks and then calling upon the banks to allow inspection of those copies without appropriate legal process." 13 Cal. 3d, at 246-247, 529 P.2d, at 595-596 (footnote omitted). [425 U.S. 435, 454]

I would therefore affirm the judgment of the Court of Appeals. I add only that Burrows strikingly illustrates the emerging trend among high state courts of relying upon state constitutional protections of individual liberties 4 - protections pervading counterpart provisions of [425 U.S. 435, 455] the United States Constitution, but increasingly being ignored by decisions of this Court. For the most recent examples in this Court, but only in the privacy and Fourth Amendment areas, see, e. g., Kelly v. Johnson, ante, p. 238; Doe v. Commonwealth's Atty., post, p. 901; Paul v. Davis, 424 U.S. 693 (1976); United States v. Watson, 423 U.S. 411 (1976).

[Footnote 1] The expectation of privacy relied upon by respondent to support his Fourth Amendment claim is similar to that rejected as to similar documents in Couch v. United States, 409 U.S. 322 (1973). But in Couch the taxpayer had delivered the documents to her accountant for preparation of income tax returns "knowing that mandatory disclosure of much of the information therein is required in an income tax return." Id., at 335; see id., at 337 (BRENNAN, J., concurring). In contrast, in the instant case the banks were obliged only to respond to lawful process, California Bankers Assn. v. Shultz, 416 U.S. 21, 52 -54 (1974), and had no obligation to disclose the information voluntarily. The expectation of privacy asserted in Fisher v. United States, ante, p. 391, is distinguishable on similar grounds.

[Footnote 2] The Court distinguishes Burrows on the ground that it involved no legal process, while the instant case involves legal process in the form of subpoenas duces tecum. Ante, at 445 n. 7. But the Court also states that the Fourth Amendment issue does not turn on whether the subpoenas were defective. Ante, at 441 n. 2.

In any event, for present purposes I would accept the Court of Appeals' conclusion that the subpoenas in this case were defective. Moreover, although not relied upon by the Court of Appeals, neither the bank nor the Government notified respondent of the disclosure of his records to the Government. In my view, the absence of such notice is not just "unattractive," ante, at 443 n. 5; a fatal constitutional defect inheres in a process that omits provision for notice to the bank customer of an invasion of his protected Fourth Amendment interest.

[Footnote 3] I continue to believe that the reporting and recordkeeping requirements of the Bank Secrecy Act are unconstitutional. California Bankers Assn. v. Shultz, 416 U.S., at 91 (BRENNAN, J., dissenting). But I disagree with the Court's reasoning in this case even assuming the constitutionality of the Act, and therefore it is unnecessary for me to rely on the infirmities inherent in the Act.

[Footnote 4] See, e. g., cases cited in Baxter v. Palmigiano, ante, at 339, and n. 10 (BRENNAN, J., dissenting); Michigan v. Mosley, 423 U.S. 96, 120 -121 (1975) (BRENNAN, J., dissenting). See also

Wilkes, The New Federalism in Criminal Procedure: State Court Evasion of the Burger Court, 62 Ky. L. J. 421 (1974); Wilkes, More on the New Federalism in Criminal Procedure, 63 Ky. L. J. 873 (1975); Falk, The State Constitution: A More Than "Adequate" Nonfederal Ground, 61 Calif. L. Rev. 273 (1973); Project Report: Toward an Activist Role for State Bills of Rights, 8 Harv. Civ. Rights-Civ. Lib. L. Rev. 271 (1973). In the past, it might have been safe for counsel to raise only federal constitutional issues in state courts, but the risks of not raising state-law questions are increasingly substantial, as revealed by a colloquy during argument in Michigan v. Mosley, supra:

> "QUESTION: Why can't you argue all of this as being contrary to the law and the Constitution of the State of Michigan?
>
> "MR. ZIEMBA: I can because we have the same provision in the Michigan Constitution of 1963 as we have in the Fifth Amendment of the Federal Constitution, certainly.
>
> . . . . .
>
> "QUESTION: Well, you argued the whole thing before.
>
> "MR. ZIEMBA: In the Court of Appeals?
>
> "QUESTION: Yes.
>
> "MR. ZIEMBA: I really did not touch upon - I predicated my entire argument on the Federal Constitution, I must admit that. I did not mention the equivalent provision of the Michigan Constitution of 1963, although I could have. And I may assure this Court that at every opportunity in the future, I shall.
>
> "[Laughter.]
>
> "QUESTION: But you hope you don't have that opportunity in this case.
>
> "MR. ZIEMBA: That's right." Tr. of Oral Arg. 43-44 (O. T. 1975, No. 74-653).

It would be unwise for counsel to rely on state courts to consider state-law questions sua sponte. But see State v. Johnson, 68 N. J. 349, 346 A. 2d 66 (1975).

MR. JUSTICE MARSHALL, dissenting.

In California Bankers Assn. v. Shultz, 416 U.S. 21 (1974), the Court upheld the constitutionality of the recordkeeping requirements of the Bank Secrecy Act. 12 U.S.C. 1829b (d). I dissented, finding the required maintenance of bank customers' records to be a seizure within the meaning of the Fourth Amendment and unlawful in the absence of a warrant and probable cause. While the Court in California Bankers Assn. did not then purport to decide whether a customer could later challenge the bank's delivery of his records to the Government pursuant to subpoena, I warned:

> "[I]t is ironic that although the majority deems the bank customers' Fourth Amendment claims premature, it also intimates that once the bank has made copies of a customer's checks, the customer no longer has standing to invoke his Fourth Amendment rights when a demand is made on the bank by the Government for the records. . . . By accepting the Government's bifurcated approach to the recordkeeping requirement and the acquisition of the records, the majority engages in a hollow charade whereby Fourth Amendment claims are to be labeled premature

until such time as they can be deemed too late." 416 U.S., at 97.

Today, not surprisingly, the Court finds respondent's claims to be made too late. Since the Court in California [425 U.S. 435, 456] Bankers Assn. held that a bank, in complying with the requirement that it keep copies of the checks written by its customers, "neither searches nor seizes records in which the depositor has a Fourth Amendment right," id., at 54, there is nothing new in today's holding that respondent has no protected Fourth Amendment interest in such records. A fortiori, he does not have standing to contest the Government's subpoena to the bank. Alderman v. United States, 394 U.S. 165 (1969).

I wash my hands of today's extended redundancy by the Court. Because the recordkeeping requirements of the Act order the seizure of customers' bank records without a warrant and probable cause, I believe the Act is unconstitutional and that respondent has standing to raise that claim. Since the Act is unconstitutional, the Government cannot rely on records kept pursuant to it in prosecuting bank customers. The Government relied on such records in this case and, because of that, I would affirm the Court of Appeals' reversal of respondent's conviction. I respectfully dissent. [425 U.S. 435, 457]

Syllabus

NOTE: Where it is feasible, a syllabus (headnote) will be released, as is being done in connection with this case, at the time the opinion is issued. The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States* v. *Detroit Timber & Lumber Co.*, 200 U. S. 321, 337.

SUPREME COURT OF THE UNITED STATES

Syllabus

KYLLO *v.* UNITED STATES

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

No. 99–8508. Argued February 20, 2001—Decided June 11, 2001

Suspicious that marijuana was being grown in petitioner Kyllo's home in a triplex, agents used a thermal imaging device to scan the triplex to determine if the amount of heat emanating from it was consistent with the high-intensity lamps typically used for indoor marijuana growth. The scan showed that Kyllo's garage roof and a side wall were relatively hot compared to the rest of his home and substantially warmer than the neighboring units. Based in part on the thermal imaging, a Federal Magistrate Judge issued a warrant to search Kyllo's home, where the agents found marijuana growing. After Kyllo was indicted on a federal drug charge, he unsuccessfully moved to suppress the evidence seized from his home and then entered a conditional guilty plea. The Ninth Circuit ultimately affirmed, upholding the thermal imaging on the ground that Kyllo had shown no subjective expectation of privacy because he had made no attempt to conceal the heat escaping from his home. Even if he had, ruled the court, there was no objectively reasonable expectation of privacy because the thermal imager did not expose any intimate details of Kyllo's life, only amorphous hot spots on his home's exterior.

Held: Where, as here, the Government uses a device that is not in general public use, to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a Fourth Amendment "search," and is presumptively unreasonable without a warrant. Pp. 3–13.

(a) The question whether a warrantless search of a home is reasonable and hence constitutional must be answered no in most instances, but the antecedent question whether a Fourth Amendment "search" has occurred is not so simple. This Court has approved warrantless visual surveillance of a home, see *California* v. *Ciraolo*, 476 U. S. 207,

213, ruling that visual observation is no "search" at all, see *Dow Chemical Co.* v. *United States*, 476 U. S. 227, 234–235, 239. In assessing when a search is not a search, the Court has adapted a principle first enunciated in *Katz* v. *United States*, 389 U. S. 347, 361: A "search" does not occur—even when its object is a house explicitly protected by the Fourth Amendment—unless the individual manifested a subjective expectation of privacy in the searched object, and society is willing to recognize that expectation as reasonable, see, *e.g.*, *California* v. *Ciraolo*, *supra*, at 211. Pp. 3–5.

(b) While it may be difficult to refine the *Katz* test in some instances, in the case of the search of a home's interior—the prototypical and hence most commonly litigated area of protected privacy—there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*. To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment. Thus, obtaining by sense-enhancing technology any information regarding the home's interior that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," *Silverman* v. *United States*, 365 U. S. 505, 512, constitutes a search—at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. Pp. 6–7.

(c) Based on this criterion, the information obtained by the thermal imager in this case was the product of a search. The Court rejects the Government's argument that the thermal imaging must be upheld because it detected only heat radiating from the home's external surface. Such a mechanical interpretation of the Fourth Amendment was rejected in *Katz*, where the eavesdropping device in question picked up only sound waves that reached the exterior of the phone booth to which it was attached. Reversing that approach would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home. Also rejected is the Government's contention that the thermal imaging was constitutional because it did not detect "intimate details." Such an approach would be wrong in principle because, in the sanctity of the home, *all* details are intimate details. See *e.g.*, *United States* v. *Karo*, 468 U. S. 705; *Dow Chemical*, *supra*, at 238, distinguished. It would also be impractical in application, failing to provide a workable accommodation between law enforcement needs and Fourth Amendment interests. See *Oliver* v. *United States*, 466 U. S. 170, 181. Pp. 7–12.

(d) Since the imaging in this case was an unlawful search, it will

Syllabus

remain for the District Court to determine whether, without the evidence it provided, the search warrant was supported by probable cause—and if not, whether there is any other basis for supporting admission of that evidence. Pp. 12–13.

190 F. 3d 1041, reversed and remanded.

SCALIA, J., delivered the opinion of the Court, in which SOUTER, THOMAS, GINSBURG, and BREYER, JJ., joined. STEVENS, J., filed a dissenting opinion, in which REHNQUIST, C. J., and O'CONNOR and KENNEDY, JJ., joined.

respect, it operates somewhat like a video camera showing heat images. The scan of Kyllo's home took only a few minutes and was performed from the passenger seat of Agent Elliott's vehicle across the street from the front of the house and also from the street in back of the house. The scan showed that the roof over the garage and a side wall of petitioner's home were relatively hot compared to the rest of the home and substantially warmer than neighboring homes in the triplex. Agent Elliott concluded that petitioner was using halide lights to grow marijuana in his house, which indeed he was. Based on tips from informants, utility bills, and the thermal imaging, a Federal Magistrate Judge issued a warrant authorizing a search of petitioner's home, and the agents found an indoor growing operation involving more than 100 plants. Petitioner was indicted on one count of manufacturing marijuana, in violation of 21 U. S. C. §841(a)(1). He unsuccessfully moved to suppress the evidence seized from his home and then entered a conditional guilty plea.

The Court of Appeals for the Ninth Circuit remanded the case for an evidentiary hearing regarding the intrusiveness of thermal imaging. On remand the District Court found that the Agema 210 "is a non-intrusive device which emits no rays or beams and shows a crude visual image of the heat being radiated from the outside of the house"; it "did not show any people or activity within the walls of the structure"; "[t]he device used cannot penetrate walls or windows to reveal conversations or human activities"; and "[n]o intimate details of the home were observed." Supp. App. to Pet. for Cert. 39–40. Based on these findings, the District Court upheld the validity of the warrant that relied in part upon the thermal imaging, and reaffirmed its denial of the motion to suppress. A divided Court of Appeals initially reversed, 140 F. 3d 1249 (1998), but that opinion was withdrawn and the panel (after a change in composition) affirmed, 190 F. 3d 1041

SUPREME COURT OF THE UNITED STATES

No. 99–8508

DANNY LEE KYLLO, PETITIONER *v.* UNITED STATES

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

[June 11, 2001]

JUSTICE SCALIA delivered the opinion of the Court.

This case presents the question whether the use of a thermal-imaging device aimed at a private home from a public street to detect relative amounts of heat within the home constitutes a "search" within the meaning of the Fourth Amendment.

I

In 1991 Agent William Elliott of the United States Department of the Interior came to suspect that marijuana was being grown in the home belonging to petitioner Danny Kyllo, part of a triplex on Rhododendron Drive in Florence, Oregon. Indoor marijuana growth typically requires high-intensity lamps. In order to determine whether an amount of heat was emanating from petitioner's home consistent with the use of such lamps, at 3:20 a.m. on January 16, 1992, Agent Elliott and Dan Haas used an Agema Thermovision 210 thermal imager to scan the triplex. Thermal imagers detect infrared radiation, which virtually all objects emit but which is not visible to the naked eye. The imager converts radiation into images based on relative warmth—black is cool, white is hot, shades of gray connote relative differences; in that

(1999), with Judge Noonan dissenting. The court held that petitioner had shown no subjective expectation of privacy because he had made no attempt to conceal the heat escaping from his home, *id.*, at 1046, and even if he had, there was no objectively reasonable expectation of privacy because the imager "did not expose any intimate details of Kyllo's life," only "amorphous 'hot spots' on the roof and exterior wall," *id.*, at 1047. We granted certiorari. 530 U. S. 1305 (2000).

II

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." "At the very core" of the Fourth Amendment "stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion." *Silverman* v. *United States*, 365 U. S. 505, 511 (1961). With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no. See *Illinois* v. *Rodriguez*, 497 U. S. 177, 181 (1990); *Payton* v. *New York*, 445 U. S. 573, 586 (1980).

On the other hand, the antecedent question of whether or not a Fourth Amendment "search" has occurred is not so simple under our precedent. The permissibility of ordinary visual surveillance of a home used to be clear because, well into the 20th century, our Fourth Amendment jurisprudence was tied to common-law trespass. See, *e.g.*, *Goldman* v. *United States*, 316 U. S. 129, 134–136 (1942); *Olmstead* v. *United States*, 277 U. S. 438, 464–466 (1928). Cf. *Silverman* v. *United States*, *supra*, at 510–512 (technical trespass not necessary for Fourth Amendment violation; it suffices if there is "actual intrusion into a constitutionally protected area"). Visual surveillance was unquestionably lawful because "'the eye

cannot by the laws of England be guilty of a trespass.'" *Boyd* v. *United States*, 116 U. S. 616, 628 (1886) (quoting *Entick* v. *Carrington*, 19 How. St. Tr. 1029, 95 Eng. Rep. 807 (K. B. 1765)). We have since decoupled violation of a person's Fourth Amendment rights from trespassory violation of his property, see *Rakas* v. *Illinois*, 439 U. S. 128, 143 (1978), but the lawfulness of warrantless visual surveillance of a home has still been preserved. As we observed in *California* v. *Ciraolo*, 476 U. S. 207, 213 (1986), "[t]he 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."

One might think that the new validating rationale would be that examining the portion of a house that is in plain public view, while it is a "search"[1] despite the absence of trespass, is not an "unreasonable" one under the Fourth Amendment. See *Minnesota* v. *Carter*, 525 U. S. 83, 104 (1998) (BREYER, J., concurring in judgment). But in fact we have held that visual observation is no "search" at all—perhaps in order to preserve somewhat more intact our doctrine that warrantless searches are presumptively unconstitutional. See *Dow Chemical Co.* v. *United States*, 476 U. S. 227, 234–235, 239 (1986). In assessing when a search is not a search, we have applied somewhat in reverse the principle first enunciated in *Katz* v. *United States*, 389 U. S. 347 (1967). *Katz* involved eavesdropping by means of an electronic listening device placed on the outside of a telephone booth—a location not within the catalog ("persons, houses, papers, and effects") that the

---

[1]When the Fourth Amendment was adopted, as now, to "search" meant "[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as, to *search* the house for a book; to *search* the wood for a thief." N. Webster, An American Dictionary of the English Language 66 (1828) (reprint 6th ed. 1989).

Fourth Amendment protects against unreasonable searches. We held that the Fourth Amendment nonetheless protected Katz from the warrantless eavesdropping because he "justifiably relied" upon the privacy of the telephone booth. *Id.*, at 353. As Justice Harlan's oft-quoted concurrence described it, a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable. See *id.*, at 361. We have subsequently applied this principle to hold that a Fourth Amendment search does *not* occur—even when the explicitly protected location of a *house* is concerned—unless "the individual manifested a subjective expectation of privacy in the object of the challenged search," and "society [is] willing to recognize that expectation as reasonable." *Ciraolo*, *supra*, at 211. We have applied this test in holding that it is not a search for the police to use a pen register at the phone company to determine what numbers were dialed in a private home, *Smith* v. *Maryland*, 442 U. S. 735, 743–744 (1979), and we have applied the test on two different occasions in holding that aerial surveillance of private homes and surrounding areas does not constitute a search, *Ciraolo*, *supra*; *Florida* v. *Riley*, 488 U. S. 445 (1989).

The present case involves officers on a public street engaged in more than naked-eye surveillance of a home. We have previously reserved judgment as to how much technological enhancement of ordinary perception from such a vantage point, if any, is too much. While we upheld enhanced aerial photography of an industrial complex in *Dow Chemical*, we noted that we found "it important that this is *not* an area immediately adjacent to a private home, where privacy expectations are most heightened," 476 U. S., at 237, n. 4 (emphasis in original).

III

It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology. For example, as the cases discussed above make clear, the technology enabling human flight has exposed to public view (and hence, we have said, to official observation) uncovered portions of the house and its curtilage that once were private. See *Ciraolo*, *supra*, at 215. The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.

The *Katz* test—whether the individual has an expectation of privacy that society is prepared to recognize as reasonable—has often been criticized as circular, and hence subjective and unpredictable. See 1 W. LaFave, Search and Seizure §2.1(d), pp. 393–394 (3d ed. 1996); Posner, The Uncertain Protection of Privacy by the Supreme Court, 1979 S. Ct. Rev. 173, 188; *Carter*, *supra*, at 97 (SCALIA, J., concurring). But see *Rakas*, *supra*, at 143–144, n. 12. While it may be difficult to refine *Katz* when the search of areas such as telephone booths, automobiles, or even the curtilage and uncovered portions of residences are at issue, in the case of the search of the interior of homes—the prototypical and hence most commonly litigated area of protected privacy—there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*. To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment. We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," *Silverman*, 365 U. S., at 512, constitutes a search—at least where (as here) the technology in question is not in general public

And, of course, the novel proposition that inference insulates a search is blatantly contrary to *United States* v. *Karo*, 468 U. S. 705 (1984), where the police "inferred" from the activation of a beeper that a certain can of ether was in the home. The police activity was held to be a search, and the search was held unlawful.[4]

The Government also contends that the thermal imaging was constitutional because it did not "detect private activities occurring in private areas," Brief for United States 22. It points out that in *Dow Chemical* we observed that the enhanced aerial photography did not reveal any "intimate details." 476 U. S., at 238. *Dow Chemical*, however, involved enhanced aerial photography of an industrial complex, which does not share the Fourth Amendment sanctity of the home. The Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained. In *Silverman*, for example, we made clear that any physical invasion of the structure of the home, "by even a fraction of an inch," was too much, 365 U. S., at 512, and there is certainly no exception to the warrant requirement for the officer who barely cracks open the

---

[4]The dissent asserts, *post*, at 5, n. 3, that we have misunderstood its point, which is not that inference *insulates* a search, but that inference alone is *not* a search. If we misunderstood the point, it was only in a good-faith effort to render the point germane to the case at hand. The issue in this case is not the police's allegedly unlawful inferencing, but their allegedly unlawful thermal-imaging measurement of the emanations from a house. We say such measurement is a search; the dissent says it is not, because an inference is not a search. We took that to mean that, since the technologically enhanced emanations had to be the basis of inferences before anything inside the house could be known, the use of the emanations could not be a search. But the dissent certainly knows better than we what it intends. And if it means only that an inference is not a search, we certainly agree. That has no bearing, however, upon whether hi-tech measurement of emanations from a house is a search.

front door and sees nothing but the nonintimate rug on the vestibule floor. In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes. Thus, in *Karo*, *supra*, the only thing detected was a can of ether in the home; and in *Arizona* v. *Hicks*, 480 U. S. 321 (1987), the only thing detected by a physical search that went beyond what officers lawfully present could observe in "plain view" was the registration number of a phonograph turntable. These were intimate details because they were details of the home, just as was the detail of how warm—or even how relatively warm—Kyllo was heating his residence.[5]

Limiting the prohibition of thermal imaging to "intimate details" would not only be wrong in principle; it would be impractical in application, failing to provide "a workable accommodation between the needs of law enforcement and the interests protected by the Fourth Amendment," *Oliver* v. *United States*, 466 U. S. 170, 181 (1984). To begin with, there is no necessary connection between the sophistication of the surveillance equipment and the "intimacy" of the details that it observes—which means that one cannot say (and the police cannot be assured) that use of the relatively crude equipment at issue here will always be lawful. The Agema Thermovision 210 might disclose, for example, at what hour each night the lady of the house takes her daily sauna and bath—a detail that many would consider "intimate"; and a much more sophisticated sys-

[5]The Government cites our statement in *California* v. *Ciraolo*, 476 U. S. 207 (1986), noting apparent agreement with the State of California that aerial surveillance of a house's curtilage could become "'invasive'" if "'modern technology'" revealed "'those intimate associations, objects or activities otherwise imperceptible to police or fellow citizens.'" *Id.*, at 215, n. 3 (quoting brief of the State of California). We think the Court's focus in this second-hand dictum was not upon intimacy but upon otherwise-imperceptibility, which is precisely the principle we vindicate today.

tem might detect nothing more intimate than the fact that someone left a closet light on. We could not, in other words, develop a rule approving only that through-the-wall surveillance which identifies objects no smaller than 36 by 36 inches, but would have to develop a jurisprudence specifying which home activities are "intimate" and which are not. And even when (if ever) that jurisprudence were fully developed, no police officer would be able to know *in advance* whether his through-the-wall surveillance picks up "intimate" details—and thus would be unable to know in advance whether it is constitutional.

The dissent's proposed standard—whether the technology offers the "functional equivalent of actual presence in the area being searched," *post*, at 7—would seem quite similar to our own at first blush. The dissent concludes that *Katz* was such a case, but then inexplicably asserts that if the same listening device only revealed the volume of the conversation, the surveillance would be permissible, *post*, at 10. Yet if, without technology, the police could not discern volume without being actually present in the phone booth, JUSTICE STEVENS should conclude a search has occurred. Cf. *Karo, supra*, at 735 (STEVENS, J., concurring in part and dissenting in part) ("I find little comfort in the Court's notion that no invasion of privacy occurs until a listener obtains some significant information by use of the device. . . . A bathtub is a less private area when the plumber is present even if his back is turned"). The same should hold for the interior heat of the home if only a person present in the home could discern the heat. Thus the driving force of the dissent, despite its recitation of the above standard, appears to be a distinction among different types of information—whether the "homeowner would even care if anybody noticed," *post*, at 10. The dissent offers no practical guidance for the application of this standard, and for reasons already discussed, we believe there can be none. The people in their houses, as

well as the police, deserve more precision.[6]

We have said that the Fourth Amendment draws "a firm line at the entrance to the house," *Payton*, 445 U. S., at 590. That line, we think, must be not only firm but also bright—which requires clear specification of those methods of surveillance that require a warrant. While it is certainly possible to conclude from the videotape of the thermal imaging that occurred in this case that no "significant" compromise of the homeowner's privacy has occurred, we must take the long view, from the original meaning of the Fourth Amendment forward.

> "The Fourth Amendment is to be construed in the light of what was deemed an unreasonable search and seizure when it was adopted, and in a manner which will conserve public interests as well as the interests and rights of individual citizens." *Carroll* v. *United States*, 267 U. S. 132, 149 (1925).

Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a "search" and is presumptively unreasonable without a warrant.

Since we hold the Thermovision imaging to have been an unlawful search, it will remain for the District Court to determine whether, without the evidence it provided, the

---

[6]The dissent argues that we have injected potential uncertainty into the constitutional analysis by noting that whether or not the technology is in general public use may be a factor. See *post*, at 7–8. That quarrel, however, is not with us but with this Court's precedent. See *Ciraolo*, *supra*, at 215 ("In an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet"). Given that we can quite confidently say that thermal imaging is not "routine," we decline in this case to reexamine that factor.

search warrant issued in this case was supported by probable cause—and if not, whether there is any other basis for supporting admission of the evidence that the search pursuant to the warrant produced.

* * *

The judgment of the Court of Appeals is reversed; the case is remanded for further proceedings consistent with this opinion.

It is so ordered.

SUPREME COURT OF THE UNITED STATES

No. 99–8508

DANNY LEE KYLLO, PETITIONER *v.* UNITED STATES

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

[June 11, 2001]

JUSTICE STEVENS, with whom THE CHIEF JUSTICE, JUSTICE O'CONNOR, and JUSTICE KENNEDY join, dissenting.

There is, in my judgment, a distinction of constitutional magnitude between "through-the-wall surveillance" that gives the observer or listener direct access to information in a private area, on the one hand, and the thought processes used to draw inferences from information in the public domain, on the other hand. The Court has crafted a rule that purports to deal with direct observations of the inside of the home, but the case before us merely involves indirect deductions from "off-the-wall" surveillance, that is, observations of the exterior of the home. Those observations were made with a fairly primitive thermal imager that gathered data exposed on the outside of petitioner's home but did not invade any constitutionally protected interest in privacy.[1] Moreover, I believe that the supposedly "bright-line" rule the Court has created in response to

[1] After an evidentiary hearing, the District Court found:
"[T]he use of the thermal imaging device here was not an intrusion into Kyllo's home. No intimate details of the home were observed, and there was no intrusion upon the privacy of the individuals within the home. The device used cannot penetrate walls or windows to reveal conversations or human activities. The device recorded only the heat being emitted from the home." Supp. App. to Pet. for Cert. 40.

its concerns about future technological developments is unnecessary, unwise, and inconsistent with the Fourth Amendment.

I

There is no need for the Court to craft a new rule to decide this case, as it is controlled by established principles from our Fourth Amendment jurisprudence. One of those core principles, of course, is that "searches and seizures *inside a home* without a warrant are presumptively unreasonable." *Payton* v. *New York*, 445 U. S. 573, 586 (1980) (emphasis added). But it is equally well settled that searches and seizures of property in plain view are presumptively reasonable. See *id.*, at 586–587.[2] Whether that property is residential or commercial, the basic principle is the same: "'What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.'" *California* v. *Ciraolo*, 476 U. S. 207, 213 (1986) (quoting *Katz* v. *United States*, 389 U. S. 347, 351 (1967)); see *Florida* v. *Riley*, 488 U. S. 445, 449–450 (1989); *California* v. *Greenwood*, 486 U. S. 35, 40–41 (1988); *Dow Chemical Co.* v. *United States*, 476 U. S. 227, 235–236 (1986); *Air Pollution Variance Bd. of Colo.* v. *Western Alfalfa Corp.*, 416 U. S. 861, 865 (1974). That is the principle implicated here.

---

[2] Thus, for example, we have found consistent with the Fourth Amendment, even absent a warrant, the search and seizure of garbage left for collection outside the curtilage of a home, *California* v. *Greenwood*, 486 U. S. 35 (1988); the aerial surveillance of a fenced-in backyard from an altitude of 1,000 feet, *California* v. *Ciraolo*, 476 U. S. 207 (1986); the aerial observation of a partially exposed interior of a residential greenhouse from 400 feet above, *Florida* v. *Riley*, 488 U. S. 445 (1989); the aerial photography of an industrial complex from several thousand feet above, *Dow Chemical Co.* v. *United States*, 476 U. S. 227 (1986); and the observation of smoke emanating from chimney stacks, *Air Pollution Variance Bd. of Colo.* v. *Western Alfalfa Corp.*, 416 U. S. 861 (1974).

While the Court "take[s] the long view" and decides this case based largely on the potential of yet-to-be-developed technology that might allow "through-the-wall surveillance," *ante*, at 11–12; see *ante*, at 8, n. 3, this case involves nothing more than off-the-wall surveillance by law enforcement officers to gather information exposed to the general public from the outside of petitioner's home. All that the infrared camera did in this case was passively measure heat emitted from the exterior surfaces of petitioner's home; all that those measurements showed were relative differences in emission levels, vaguely indicating that some areas of the roof and outside walls were warmer than others. As still images from the infrared scans show, see Appendix, *infra*, no details regarding the interior of petitioner's home were revealed. Unlike an x-ray scan, or other possible "through-the-wall" techniques, the detection of infrared radiation emanating from the home did not accomplish "an unauthorized physical penetration into the premises," *Silverman* v. *United States*, 365 U. S. 505, 509 (1961), nor did it "obtain information that it could not have obtained by observation from outside the curtilage of the house," *United States* v. *Karo*, 468 U. S. 705, 715 (1984).

Indeed, the ordinary use of the senses might enable a neighbor or passerby to notice the heat emanating from a building, particularly if it is vented, as was the case here. Additionally, any member of the public might notice that one part of a house is warmer than another part or a nearby building if, for example, rainwater evaporates or snow melts at different rates across its surfaces. Such use of the senses would not convert into an unreasonable search if, instead, an adjoining neighbor allowed an officer onto her property to verify her perceptions with a sensitive thermometer. Nor, in my view, does such observation become an unreasonable search if made from a distance with the aid of a device that merely discloses that the

exterior of one house, or one area of the house, is much warmer than another. Nothing more occurred in this case.

Thus, the notion that heat emissions from the outside of a dwelling is a private matter implicating the protections of the Fourth Amendment (the text of which guarantees the right of people "to be secure *in* their . . . houses" against unreasonable searches and seizures (emphasis added)) is not only unprecedented but also quite difficult to take seriously. Heat waves, like aromas that are generated in a kitchen, or in a laboratory or opium den, enter the public domain if and when they leave a building. A subjective expectation that they would remain private is not only implausible but also surely not "one that society is prepared to recognize as 'reasonable.'" *Katz*, 389 U. S., at 361 (Harlan, J., concurring).

To be sure, the homeowner has a reasonable expectation of privacy concerning what takes place within the home, and the Fourth Amendment's protection against physical invasions of the home should apply to their functional equivalent. But the equipment in this case did not penetrate the walls of petitioner's home, and while it did pick up "details of the home" that were exposed to the public, *ante*, at 10, it did not obtain "any information regarding the *interior* of the home," *ante*, at 6 (emphasis added). In the Court's own words, based on what the thermal imager "showed" regarding the outside of petitioner's home, the officers "concluded" that petitioner was engaging in illegal activity inside the home. *Ante*, at 2. It would be quite absurd to characterize their thought processes as "searches," regardless of whether they inferred (rightly) that petitioner was growing marijuana in his house, or (wrongly) that "the lady of the house [was taking] her daily sauna and bath." *Ante*, at 10–11. In either case, the only conclusions the officers reached concerning the interior of the home were at least as indirect as those that might have been inferred from the contents of discarded

garbage, see *California* v. *Greenwood,* 486 U. S. 35 (1988), or pen register data, see *Smith* v. *Maryland,* 442 U. S. 735 (1979), or, as in this case, subpoenaed utility records, see 190 F. 3d 1041, 1043 (CA9 1999). For the first time in its history, the Court assumes that an inference can amount to a Fourth Amendment violation. See *ante,* at 8.[3]

Notwithstanding the implications of today's decision, there is a strong public interest in avoiding constitutional litigation over the monitoring of emissions from homes, and over the inferences drawn from such monitoring. Just as "the police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public," *Greenwood,* 486 U. S., at 41, so too public officials should not have to avert their senses or their equipment from detecting emissions in the public domain such as excessive heat, traces of smoke, suspicious odors, odorless gases, airborne particulates, or radioactive emissions, any of which could identify hazards to the community. In my judgment, monitoring such emissions with "sense-enhancing technology," *ante,* at 6, and drawing useful conclusions from such monitoring, is an entirely reasonable public service.

On the other hand, the countervailing privacy interest is at best trivial. After all, homes generally are insulated to

---

[3]Although the Court credits us with the "novel proposition that inference insulates a search," *ante,* at 9, our point simply is that an inference cannot *be* a search, contrary to the Court's reasoning. See *supra,* at 4–5. Thus, the Court's use of *United States* v. *Karo,* 468 U. S. 705 (1984), to refute a point we do not make underscores the fact that the Court has no real answer (either in logic or in law) to the point we do make. Of course, *Karo* itself does not provide any support for the Court's view that inferences can amount to unconstitutional searches. The illegality in that case was "the monitoring of a beeper in a private residence" to obtain information that "could not have been obtained by observation from outside," *id.,* at 714–715, rather than any thought processes that flowed from such monitoring.

keep heat in, rather than to prevent the detection of heat going out, and it does not seem to me that society will suffer from a rule requiring the rare homeowner who both intends to engage in uncommon activities that produce extraordinary amounts of heat, and wishes to conceal that production from outsiders, to make sure that the surrounding area is well insulated. Cf. *United States* v. *Jacobsen*, 466 U. S. 109, 122 (1984) ("The concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation, however well justified, that certain facts will not come to the attention of the authorities"). The interest in concealing the heat escaping from one's house pales in significance to the "the chief evil against which the wording of the Fourth Amendment is directed," the "physical entry of the home," *United States* v. *United States Dist. Court for Eastern Dist. of Mich.*, 407 U. S. 297, 313 (1972), and it is hard to believe that it is an interest the Framers sought to protect in our Constitution.

Since what was involved in this case was nothing more than drawing inferences from off-the-wall surveillance, rather than any "through-the-wall" surveillance, the officers' conduct did not amount to a search and was perfectly reasonable.[4]

II

Instead of trying to answer the question whether the

---

[4]This view comports with that of all the Courts of Appeals that have resolved the issue. See 190 F. 3d 1041 (CA9 1999); *United States* v. *Robinson*, 62 F. 3d 1325 (CA11 1995) (upholding warrantless use of thermal imager); *United States* v. *Myers*, 46 F. 3d 668 (CA7 1995) (same); *United States* v. *Ishmael*, 48 F. 3d 850 (CA5 1995) (same); *United States* v. *Pinson*, 24 F. 3d 1056 (CA8 1994) (same). But see *United States* v. *Cusumano*, 67 F. 3d 1497 (CA10 1995) (warrantless use of thermal imager violated Fourth Amendment), vacated and decided on other grounds, 83 F. 3d 1247 (CA10 1996) (en banc).

use of the thermal imager in this case was even arguably unreasonable, the Court has fashioned a rule that is intended to provide essential guidance for the day when "more sophisticated systems" gain the "ability to 'see' through walls and other opaque barriers." *Ante*, at 8, and n. 3. The newly minted rule encompasses "obtaining [1] by sense-enhancing technology [2] any information regarding the interior of the home [3] that could not otherwise have been obtained without physical intrusion into a constitutionally protected area . . . [4] at least where (as here) the technology in question is not in general public use." *Ante*, at 6–7 (internal quotation marks omitted). In my judgment, the Court's new rule is at once too broad and too narrow, and is not justified by the Court's explanation for its adoption. As I have suggested, I would not erect a constitutional impediment to the use of sense-enhancing technology unless it provides its user with the functional equivalent of actual presence in the area being searched.

Despite the Court's attempt to draw a line that is "not only firm but also bright," *ante*, at 12, the contours of its new rule are uncertain because its protection apparently dissipates as soon as the relevant technology is "in general public use," *ante*, at 6–7. Yet how much use is general public use is not even hinted at by the Court's opinion, which makes the somewhat doubtful assumption that the thermal imager used in this case does not satisfy that criterion.[5] In any event, putting aside its lack of clarity,

[5]The record describes a device that numbers close to a thousand manufactured units; that has a predecessor numbering in the neighborhood of 4,000 to 5,000 units; that competes with a similar product numbering from 5,000 to 6,000 units; and that is "readily available to the public" for commercial, personal, or law enforcement purposes, and is just an 800-number away from being rented from "half a dozen national companies" by anyone who wants one. App. 18. Since, by virtue of the Court's new rule, the issue is one of first impression, perhaps it should order an evidentiary hearing to determine whether

this criterion is somewhat perverse because it seems likely that the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available.

It is clear, however, that the category of "sense-enhancing technology" covered by the new rule, *ante*, at 6, is far too broad. It would, for example, embrace potential mechanical substitutes for dogs trained to react when they sniff narcotics. But in *United States* v. *Place*, 462 U. S. 696, 707 (1983), we held that a dog sniff that "discloses only the presence or absence of narcotics" does "not constitute a 'search' within the meaning of the Fourth Amendment," and it must follow that sense-enhancing equipment that identifies nothing but illegal activity is not a search either. Nevertheless, the use of such a device would be unconstitutional under the Court's rule, as would the use of other new devices that might detect the odor of deadly bacteria or chemicals for making a new type of high explosive, even if the devices (like the dog sniffs) are "so limited in both the manner in which" they obtain information and "in the content of the information" they reveal. *Ibid.* If nothing more than that sort of information could be obtained by using the devices in a public place to monitor emissions from a house, then their use would be no more objectionable than the use of the thermal imager in this case.

The application of the Court's new rule to "any information regarding the interior of the home," *ante*, at 6, is also unnecessarily broad. If it takes sensitive equipment to detect an odor that identifies criminal conduct and nothing else, the fact that the odor emanates from the interior of a home should not provide it with constitutional protection. See *supra*, at 7–8. The criterion, moreover, is too sweeping in that information "regarding" the interior of a

---

these facts suffice to establish "general public use."

home apparently is not just information obtained through its walls, but also information concerning the outside of the building that could lead to (however many) inferences "regarding" what might be inside. Under that expansive view, I suppose, an officer using an infrared camera to observe a man silently entering the side door of a house at night carrying a pizza might conclude that its interior is now occupied by someone who likes pizza, and by doing so the officer would be guilty of conducting an unconstitutional "search" of the home.

Because the new rule applies to information regarding the "interior" of the home, it is too narrow as well as too broad. Clearly, a rule that is designed to protect individuals from the overly intrusive use of sense-enhancing equipment should not be limited to a home. If such equipment did provide its user with the functional equivalent of access to a private place—such as, for example, the telephone booth involved in *Katz*, or an office building—then the rule should apply to such an area as well as to a home. See *Katz*, 389 U. S., at 351 ("[T]he Fourth Amendment protects people, not places").

The final requirement of the Court's new rule, that the information "could not otherwise have been obtained without physical intrusion into a constitutionally protected area," *ante*, at 6 (internal quotation marks omitted), also extends too far as the Court applies it. As noted, the Court effectively treats the mental process of analyzing data obtained from external sources as the equivalent of a physical intrusion into the home. See *supra*, at 4–5. As I have explained, however, the process of drawing inferences from data in the public domain should not be characterized as a search.

The two reasons advanced by the Court as justifications for the adoption of its new rule are both unpersuasive. First, the Court suggests that its rule is compelled by our holding in *Katz*, because in that case, as in this, the sur-

veillance consisted of nothing more than the monitoring of waves emanating from a private area into the public domain. See *ante*, at 7–8. Yet there are critical differences between the cases. In *Katz*, the electronic listening device attached to the outside of the phone booth allowed the officers to pick up the content of the conversation inside the booth, making them the functional equivalent of intruders because they gathered information that was otherwise available only to someone inside the private area; it would be as if, in this case, the thermal imager presented a view of the heat-generating activity inside petitioner's home. By contrast, the thermal imager here disclosed only the relative amounts of heat radiating from the house; it would be as if, in *Katz*, the listening device disclosed only the relative volume of sound leaving the booth, which presumably was discernible in the public domain.[6] Surely, there is a significant difference between the general and well-settled expectation that strangers will not have direct access to the contents of private communications, on the one hand, and the rather theoretical expectation that an occasional homeowner would even care if anybody noticed the relative amounts of heat emanating from the walls of his house, on the other. It is pure hyperbole for the Court to suggest that refusing to extend the holding of *Katz* to this case would leave the homeowner at the mercy of "technology that could discern all human activity in the home." *Ante*, at 8.

Second, the Court argues that the permissibility of "through-the-wall surveillance" cannot depend on a distinction between observing "intimate details" such as "the

---

[6] The use of the latter device would be constitutional given *Smith* v. *Maryland*, 442 U. S. 735, 741 (1979), which upheld the use of pen registers to record numbers dialed on a phone because, unlike "the listening device employed in *Katz* . . . pen registers do not acquire the *contents* of communications."

lady of the house [taking] her daily sauna and bath," and noticing only "the nonintimate rug on the vestibule floor" or "objects no smaller than 36 by 36 inches." *Ante*, at 10–11. This entire argument assumes, of course, that the thermal imager in this case could or did perform "through-the-wall surveillance" that could identify any detail "that would previously have been unknowable without physical intrusion." *Ante*, at 11–12. In fact, the device could not, see n. 1, *supra*, and did not, see Appendix, *infra*, enable its user to identify either the lady of the house, the rug on the vestibule floor, or anything else inside the house, whether smaller or larger than 36 by 36 inches. Indeed, the vague thermal images of petitioner's home that are reproduced in the Appendix were submitted by him to the District Court as part of an expert report raising the question whether the device could even take "accurate, consistent infrared images" of the *outside* of his house. Defendant's Exhibit 107, p. 4. But even if the device could reliably show extraordinary differences in the amounts of heat leaving his home, drawing the inference that there was something suspicious occurring inside the residence—a conclusion that officers far less gifted than Sherlock Holmes would readily draw—does not qualify as "through-the-wall surveillance," much less a Fourth Amendment violation.

III

Although the Court is properly and commendably concerned about the threats to privacy that may flow from advances in the technology available to the law enforcement profession, it has unfortunately failed to heed the tried and true counsel of judicial restraint. Instead of concentrating on the rather mundane issue that is actually presented by the case before it, the Court has endeavored to craft an all-encompassing rule for the future. It would be far wiser to give legislators an unimpeded oppor-

tunity to grapple with these emerging issues rather than to shackle them with prematurely devised constitutional constraints.

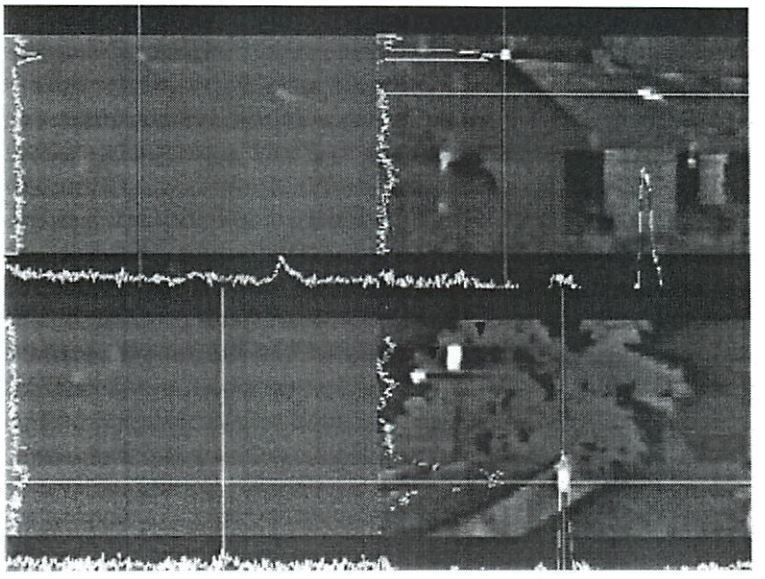
I respectfully dissent.

APPENDIX

(Images and text reproduced from defendant's exhibit 107)

Top left: Infrared image of a video frame from the videotape submitted as evidence in this case. The thermogram indicates the suspect house as it appeared with the Gain and contrast in its default setting. Only the outline of the house is visible. The camera used was the Thermovision 210.

Top Right: Infrared image of a subsequent videoframe taken from the videotape. The gain and contrast settings have been increased in order to make the walls and roof of the structure appear hotter than what it actually is.



Bottom Left: Infrared image of the opposite side of the suspects house. The thermogram is also taken from the same videotape. The camera settings are in the default mode and the outline of the house is barely visible. Only the hot electrical transformer and the street light are identifiable.

Bottom Right: The same image, but with the gain and contrast increased. This change in camera settings cause any object to appear hotter than what it actually is. The arrow indicates the overloading of a area immediately around a hot object in this case the electrical transformer and the streetlight. This overloading of the image is a inherent design flaw in the camera itself.

Read 10/18 intro

Syllabus

NOTE: Where it is feasible, a syllabus (headnote) will be released, as is being done in connection with this case, at the time the opinion is issued. The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States* v. *Detroit Timber & Lumber Co.*, 200 U. S. 321, 337.

SUPREME COURT OF THE UNITED STATES

Syllabus

UNITED STATES *v.* JONES

CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

No. 10–1259. Argued November 8, 2011—Decided January 23, 2012

The Government obtained a search warrant permitting it to install a Global-Positioning-System (GPS) tracking device on a vehicle registered to respondent Jones's wife. The warrant authorized installation in the District of Columbia and within 10 days, but agents installed the device on the 11th day and in Maryland. The Government then tracked the vehicle's movements for 28 days. It subsequently secured an indictment of Jones and others on drug trafficking conspiracy charges. The District Court suppressed the GPS data obtained while the vehicle was parked at Jones's residence, but held the remaining data admissible because Jones had no reasonable expectation of privacy when the vehicle was on public streets. Jones was convicted. The D. C. Circuit reversed, concluding that admission of the evidence obtained by warrantless use of the GPS device violated the Fourth Amendment.

< what — > point less

Held: The Government's attachment of the GPS device to the vehicle, and its use of that device to monitor the vehicle's movements, constitutes a search under the Fourth Amendment. Pp. 3–12.

(a) The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." Here, the Government's physical intrusion on an "effect" for the purpose of obtaining information constitutes a "search." This type of encroachment on an area enumerated in the Amendment would have been considered a search within the meaning of the Amendment at the time it was adopted. Pp. 3–4.

(b) This conclusion is consistent with this Court's Fourth Amendment jurisprudence, which until the latter half of the 20th century was tied to common-law trespass. Later cases, which have deviated from that exclusively property-based approach, have applied the

Syllabus

analysis of Justice Harlan's concurrence in *Katz* v. *United States*, 389 U. S. 347, which said that the Fourth Amendment protects a person's "reasonable expectation of privacy," *id.*, at 360. Here, the Court need not address the Government's contention that Jones had no "reasonable expectation of privacy," because Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation. At bottom, the Court must "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo* v. *United States*, 533 U. S. 27, 34. *Katz* did not repudiate the understanding that the Fourth Amendment embodies a particular concern for government trespass upon the areas it enumerates. The *Katz* reasonable-expectation-of-privacy test has been added to, but not substituted for, the common-law trespassory test. See *Alderman* v. *United States*, 394 U. S. 165, 176; *Soldal* v. *Cook County*, 506 U. S. 56, 64. *United States* v. *Knotts*, 460 U. S. 276, and *United States* v. *Karo*, 468 U. S. 705—post-*Katz* cases rejecting Fourth Amendment challenges to "beepers," electronic tracking devices representing another form of electronic monitoring—do not foreclose the conclusion that a search occurred here. *New York* v. *Class*, 475 U. S. 106, and *Oliver* v. *United States*, 466 U. S. 170, also do not support the Government's position. Pp. 4–12.

(c) The Government's alternative argument—that if the attachment and use of the device was a search, it was a reasonable one—is forfeited because it was not raised below. P. 12.

615 F. 3d 544, affirmed.

SCALIA, J., delivered the opinion of the Court, in which ROBERTS, C. J., and KENNEDY, THOMAS, and SOTOMAYOR, JJ., joined. SOTOMAYOR, J., filed a concurring opinion. ALITO, J., filed an opinion concurring in the judgment, in which GINSBURG, BREYER, and KAGAN, JJ., joined.

SUPREME COURT OF THE UNITED STATES

No. 10–1259

UNITED STATES, PETITIONER *v.* ANTOINE JONES

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

[January 23, 2012]

JUSTICE SCALIA delivered the opinion of the Court.

We decide whether the attachment of a Global-Positioning-System (GPS) tracking device to an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets, constitutes a search or seizure within the meaning of the Fourth Amendment.

I

In 2004 respondent Antoine Jones, owner and operator of a nightclub in the District of Columbia, came under suspicion of trafficking in narcotics and was made the target of an investigation by a joint FBI and Metropolitan Police Department task force. Officers employed various investigative techniques, including visual surveillance of the nightclub, installation of a camera focused on the front door of the club, and a pen register and wiretap covering Jones's cellular phone.

Based in part on information gathered from these sources, in 2005 the Government applied to the United States District Court for the District of Columbia for a warrant authorizing the use of an electronic tracking device on the Jeep Grand Cherokee registered to Jones's

wife. A warrant issued, authorizing installation of the device in the District of Columbia and within 10 days.

On the 11th day, and not in the District of Columbia but in Maryland,[1] agents installed a GPS tracking device on the undercarriage of the Jeep while it was parked in a public parking lot. Over the next 28 days, the Government used the device to track the vehicle's movements, and once had to replace the device's battery when the vehicle was parked in a different public lot in Maryland. By means of signals from multiple satellites, the device established the vehicle's location within 50 to 100 feet, and communicated that location by cellular phone to a Government computer. It relayed more than 2,000 pages of data over the 4-week period.

The Government ultimately obtained a multiple-count indictment charging Jones and several alleged coconspirators with, as relevant here, conspiracy to distribute and possess with intent to distribute five kilograms or more of cocaine and 50 grams or more of cocaine base, in violation of 21 U. S. C. §§841 and 846. Before trial, Jones filed a motion to suppress evidence obtained through the GPS device. The District Court granted the motion only in part, suppressing the data obtained while the vehicle was parked in the garage adjoining Jones's residence. 451 F. Supp. 2d 71, 88 (2006). It held the remaining data admissible, because "'[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.'" *Ibid.* (quoting *United States* v. *Knotts*, 460 U. S. 276, 281 (1983)). Jones's trial in October 2006 produced a hung jury on the conspiracy count.

In March 2007, a grand jury returned another indict-

---

[1] In this litigation, the Government has conceded noncompliance with the warrant and has argued only that a warrant was not required. *United States* v. *Maynard*, 615 F. 3d 544, 566, n. (CADC 2010).

ment, charging Jones and others with the same conspiracy. The Government introduced at trial the same GPS-derived locational data admitted in the first trial, which connected Jones to the alleged conspirators' stash house that contained $850,000 in cash, 97 kilograms of cocaine, and 1 kilogram of cocaine base. The jury returned a guilty verdict, and the District Court sentenced Jones to life imprisonment.

The United States Court of Appeals for the District of Columbia Circuit reversed the conviction because of admission of the evidence obtained by warrantless use of the GPS device which, it said, violated the Fourth Amendment. *United States* v. *Maynard*, 615 F. 3d 544 (2010). The D. C. Circuit denied the Government's petition for rehearing en banc, with four judges dissenting. 625 F. 3d 766 (2010). We granted certiorari, 564 U. S. ___ (2011).

II

A

The Fourth Amendment provides in relevant part that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." It is beyond dispute that a vehicle is an "effect" as that term is used in the Amendment. *United States* v. *Chadwick*, 433 U. S. 1, 12 (1977). We hold that the Government's installation of a GPS device on a target's vehicle,[2] and its use of that device to monitor the vehicle's movements, constitutes a "search."

---

[2]As we have noted, the Jeep was registered to Jones's wife. The Government acknowledged, however, that Jones was "the exclusive driver." *Id.*, at 555, n. (internal quotation marks omitted). If Jones was not the owner he had at least the property rights of a bailee. The Court of Appeals concluded that the vehicle's registration did not affect his ability to make a Fourth Amendment objection, *ibid.*, and the Government has not challenged that determination here. We therefore do not consider the Fourth Amendment significance of Jones's status.

It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted. *Entick* v. *Carrington*, 95 Eng. Rep. 807 (C. P. 1765), is a "case we have described as a 'monument of English freedom' 'undoubtedly familiar' to 'every American statesman' at the time the Constitution was adopted, and considered to be 'the true and ultimate expression of constitutional law'" with regard to search and seizure. *Brower* v. *County of Inyo*, 489 U. S. 593, 596 (1989) (quoting *Boyd* v. *United States*, 116 U. S. 616, 626 (1886)). In that case, Lord Camden expressed in plain terms the significance of property rights in search-and-seizure analysis:

> "[O]ur law holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without his leave; if he does he is a trespasser, though he does no damage at all; if he will tread upon his neighbour's ground, he must justify it by law." *Entick, supra,* at 817.

The text of the Fourth Amendment reflects its close connection to property, since otherwise it would have referred simply to "the right of the people to be secure against unreasonable searches and seizures"; the phrase "in their persons, houses, papers, and effects" would have been superfluous.

Consistent with this understanding, our Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century. *Kyllo* v. *United States*, 533 U. S. 27, 31 (2001); Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 Mich. L. Rev. 801, 816 (2004). Thus, in *Olmstead* v. *United States*, 277 U. S.

438 (1928), we held that wiretaps attached to telephone wires on the public streets did not constitute a Fourth Amendment search because "[t]here was no entry of the houses or offices of the defendants," *id.*, at 464.

Our later cases, of course, have deviated from that exclusively property-based approach. In *Katz* v. *United States*, 389 U. S. 347, 351 (1967), we said that "the Fourth Amendment protects people, not places," and found a violation in attachment of an eavesdropping device to a public telephone booth. Our later cases have applied the analysis of Justice Harlan's concurrence in that case, which said that a violation occurs when government officers violate a person's "reasonable expectation of privacy," *id.*, at 360. See, *e.g.*, *Bond* v. *United States*, 529 U. S. 334 (2000); *California* v. *Ciraolo*, 476 U. S. 207 (1986); *Smith* v. *Maryland*, 442 U. S. 735 (1979).

The Government contends that the Harlan standard shows that no search occurred here, since Jones had no "reasonable expectation of privacy" in the area of the Jeep accessed by Government agents (its underbody) and in the locations of the Jeep on the public roads, which were visible to all. But we need not address the Government's contentions, because Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation. At bottom, we must "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo*, *supra*, at 34. As explained, for most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ("persons, houses, papers, and effects") it enumerates.[3] *Katz* did not repudiate

---

[3]JUSTICE ALITO's concurrence (hereinafter concurrence) doubts the wisdom of our approach because "it is almost impossible to think of late-18th-century situations that are analogous to what took place in this case." *Post*, at 3 (opinion concurring in judgment). But in fact it posits a situation that is not far afield—a constable's concealing himself

that understanding. Less than two years later the Court upheld defendants' contention that the Government could not introduce against them conversations between *other* people obtained by warrantless placement of electronic surveillance devices in their homes. The opinion rejected the dissent's contention that there was no Fourth Amendment violation "unless the conversational privacy of the homeowner himself is invaded."[4] *Alderman* v. *United States*, 394 U. S. 165, 176 (1969). "[W]e [do not] believe that *Katz*, by holding that the Fourth Amendment protects persons and their private conversations, was intended to withdraw any of the protection which the Amendment extends to the home . . . ." *Id.*, at 180.

More recently, in *Soldal* v. *Cook County*, 506 U. S. 56 (1992), the Court unanimously rejected the argument that although a "seizure" had occurred "in a 'technical' sense" when a trailer home was forcibly removed, *id.*, at 62, no Fourth Amendment violation occurred because law enforcement had not "invade[d] the [individuals'] privacy," *id.*, at 60. *Katz*, the Court explained, established that "property rights are not the sole measure of Fourth

---

in the target's coach in order to track its movements. *Ibid.* There is no doubt that the information gained by that trespassory activity would be the product of an unlawful search—whether that information consisted of the conversations occurring in the coach, or of the destinations to which the coach traveled.

In any case, it is quite irrelevant whether there was an 18th-century analog. Whatever new methods of investigation may be devised, our task, *at a minimum*, is to decide whether the action in question would have constituted a "search" within the original meaning of the Fourth Amendment. Where, as here, the Government obtains information by physically intruding on a constitutionally protected area, such a search has undoubtedly occurred.

[4] Thus, the concurrence's attempt to recast *Alderman* as meaning that individuals have a "legitimate expectation of privacy in all conversations that [take] place under their roof," *post*, at 6–7, is foreclosed by the Court's opinion. The Court took as a given that the homeowner's "conversational privacy" had not been violated.

Amendment violations," but did not "snuf[f] out the previously recognized protection for property." 506 U. S., at 64. As Justice Brennan explained in his concurrence in *Knotts*, *Katz* did not erode the principle "that, when the Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment." 460 U. S., at 286 (opinion concurring in judgment). We have embodied that preservation of past rights in our very definition of "reasonable expectation of privacy" which we have said to be an expectation "that has a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." *Minnesota* v. *Carter*, 525 U. S. 83, 88 (1998) (internal quotation marks omitted). *Katz* did not narrow the Fourth Amendment's scope.[5]

The Government contends that several of our post-*Katz* cases foreclose the conclusion that what occurred here constituted a search. It relies principally on two cases in

---

[5]The concurrence notes that post-*Katz* we have explained that "'an actual trespass is neither necessary *nor sufficient* to establish a constitutional violation.'" *Post*, at 6 (quoting *United States* v. *Karo*, 468 U. S. 705, 713 (1984)). That is undoubtedly true, and undoubtedly irrelevant. *Karo* was considering whether a seizure occurred, and as the concurrence explains, a seizure of property occurs, not when there is a trespass, but "when there is some meaningful interference with an individual's possessory interests in that property." *Post*, at 2 (internal quotation marks omitted). Likewise with a search. Trespass alone does not qualify, but there must be conjoined with that what was present here: an attempt to find something or to obtain information.

Related to this, and similarly irrelevant, is the concurrence's point that, if analyzed separately, neither the installation of the device nor its use would constitute a Fourth Amendment search. See *ibid.* Of course not. A trespass on "houses" or "effects," or a *Katz* invasion of privacy, is not alone a search unless it is done to obtain information; and the obtaining of information is not alone a search unless it is achieved by such a trespass or invasion of privacy.

which we rejected Fourth Amendment challenges to "beepers," electronic tracking devices that represent another form of electronic monitoring. The first case, *Knotts*, upheld against Fourth Amendment challenge the use of a "beeper" that had been placed in a container of chloroform, allowing law enforcement to monitor the location of the container. 460 U. S., at 278. We said that there had been no infringement of Knotts' reasonable expectation of privacy since the information obtained—the location of the automobile carrying the container on public roads, and the location of the off-loaded container in open fields near Knotts' cabin—had been voluntarily conveyed to the public.[6] *Id.*, at 281–282. But as we have discussed, the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test. The holding in *Knotts* addressed only the former, since the latter was not at issue. The beeper had been placed in the container before it came into Knotts' possession, with the consent of the then-owner. 460 U. S., at 278. Knotts did not challenge that installation, and we specifically declined to consider its effect on the Fourth Amendment analysis. *Id.*, at 279, n. *Knotts* would be relevant, perhaps, if the Government were making the argument that what would otherwise be an unconstitutional search is not such where it produces only public information. The Government does not make that argument, and we know of no case that would support it.

The second "beeper" case, *United States* v. *Karo*, 468 U. S. 705 (1984), does not suggest a different conclusion. There we addressed the question left open by *Knotts*, whether the installation of a beeper in a container

---

[6] *Knotts* noted the "limited use which the government made of the signals from this particular beeper," 460 U. S., at 284; and reserved the question whether "different constitutional principles may be applicable" to "dragnet-type law enforcement practices" of the type that GPS tracking made possible here, *ibid.*

amounted to a search or seizure. 468 U. S., at 713. As in *Knotts*, at the time the beeper was installed the container belonged to a third party, and it did not come into possession of the defendant until later. 468 U. S., at 708. Thus, the specific question we considered was whether the installation "*with the consent of the original owner* constitute[d] a search or seizure . . . when the container is delivered to a buyer having no knowledge of the presence of the beeper." *Id.*, at 707 (emphasis added). We held not. The Government, we said, came into physical contact with the container only before it belonged to the defendant Karo; and the transfer of the container with the unmonitored beeper inside did not convey any information and thus did not invade Karo's privacy. See *id.*, at 712. That conclusion is perfectly consistent with the one we reach here. Karo accepted the container as it came to him, beeper and all, and was therefore not entitled to object to the beeper's presence, even though it was used to monitor the container's location. Cf. *On Lee* v. *United States*, 343 U. S. 747, 751–752 (1952) (no search or seizure where an informant, who was wearing a concealed microphone, was invited into the defendant's business). Jones, who possessed the Jeep at the time the Government trespassorily inserted the information-gathering device, is on much different footing.

The Government also points to our exposition in *New York* v. *Class*, 475 U. S. 106 (1986), that "[t]he exterior of a car . . . is thrust into the public eye, and thus to examine it does not constitute a 'search.'" *Id.*, at 114. That statement is of marginal relevance here since, as the Government acknowledges, "the officers in this case did *more* than conduct a visual inspection of respondent's vehicle," Brief for United States 41 (emphasis added). By attaching the device to the Jeep, officers encroached on a protected area. In *Class* itself we suggested that this would make a difference, for we concluded that an officer's momentary reaching into the interior of a vehicle did constitute a

search.[7] 475 U. S., at 114–115.

Finally, the Government's position gains little support from our conclusion in *Oliver* v. *United States*, 466 U. S. 170 (1984), that officers' information-gathering intrusion on an "open field" did not constitute a Fourth Amendment search even though it was a trespass at common law, *id.*, at 183. Quite simply, an open field, unlike the curtilage of a home, see *United States* v. *Dunn*, 480 U. S. 294, 300 (1987), is not one of those protected areas enumerated in the Fourth Amendment. *Oliver, supra*, at 176–177. See also *Hester* v. *United States*, 265 U. S. 57, 59 (1924). The Government's physical intrusion on such an area—unlike its intrusion on the "effect" at issue here—is of no Fourth Amendment significance.[8]

B

The concurrence begins by accusing us of applying "18th-century tort law." *Post*, at 1. That is a distortion. What we apply is an 18th-century guarantee against unreasonable searches, which we believe must provide *at*

---

[7]The Government also points to *Cardwell* v. *Lewis*, 417 U. S. 583 (1974), in which the Court rejected the claim that the inspection of an impounded vehicle's tire tread and the collection of paint scrapings from its exterior violated the Fourth Amendment. Whether the plurality said so because no search occurred or because the search was reasonable is unclear. Compare *id.*, at 591 (opinion of Blackmun, J.) ("[W]e fail to comprehend what expectation of privacy was infringed"), with *id.*, at 592 ("Under circumstances such as these, where probable cause exists, a warrantless examination of the exterior of a car is not unreasonable . . . ").

[8]Thus, our theory is *not* that the Fourth Amendment is concerned with "*any* technical trespass that led to the gathering of evidence." *Post*, at 3 (ALITO, J., concurring in judgment) (emphasis added). The Fourth Amendment protects against trespassory searches only with regard to those items ("persons, houses, papers, and effects") that it enumerates. The trespass that occurred in *Oliver* may properly be understood as a "search," but not one "in the constitutional sense." 466 U. S., at 170, 183.

a minimum the degree of protection it afforded when it was adopted. The concurrence does not share that belief. It would apply *exclusively Katz*'s reasonable-expectation-of-privacy test, even when that eliminates rights that previously existed.

The concurrence faults our approach for "present[ing] particularly vexing problems" in cases that do not involve physical contact, such as those that involve the transmission of electronic signals. *Post*, at 9. We entirely fail to understand that point. For unlike the concurrence, which would make *Katz* the *exclusive* test, we do not make trespass the exclusive test. Situations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis.

In fact, it is the concurrence's insistence on the exclusivity of the *Katz* test that needlessly leads us into "particularly vexing problems" in the present case. This Court has to date not deviated from the understanding that mere visual observation does not constitute a search. See *Kyllo*, 533 U. S., at 31–32. We accordingly held in *Knotts* that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." 460 U. S., at 281. Thus, even assuming that the concurrence is correct to say that "[t]raditional surveillance" of Jones for a 4-week period "would have required a large team of agents, multiple vehicles, and perhaps aerial assistance," *post*, at 12, our cases suggest that such visual observation is constitutionally permissible. It may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.

And answering it affirmatively leads us needlessly into additional thorny problems. The concurrence posits that "relatively short-term monitoring of a person's movements

on public streets" is okay, but that "the use of longer term GPS monitoring in investigations *of most offenses*" is no good. *Post*, at 13 (emphasis added). That introduces yet another novelty into our jurisprudence. There is no precedent for the proposition that whether a search has occurred depends on the nature of the crime being investigated. And even accepting that novelty, it remains unexplained why a 4-week investigation is "surely" too long and why a drug-trafficking conspiracy involving substantial amounts of cash and narcotics is not an "extraordinary offens[e]" which may permit longer observation. See *post*, at 13–14. What of a 2-day monitoring of a suspected purveyor of stolen electronics? Or of a 6-month monitoring of a suspected terrorist? We may have to grapple with these "vexing problems" in some future case where a classic trespassory search is not involved and resort must be had to *Katz* analysis; but there is no reason for rushing forward to resolve them here.

III

The Government argues in the alternative that even if the attachment and use of the device was a search, it was reasonable—and thus lawful—under the Fourth Amendment because "officers had reasonable suspicion, and indeed probable cause, to believe that [Jones] was a leader in a large-scale cocaine distribution conspiracy." Brief for United States 50–51. We have no occasion to consider this argument. The Government did not raise it below, and the D. C. Circuit therefore did not address it. See 625 F. 3d, at 767 (Ginsburg, Tatel, and Griffith, JJ., concurring in denial of rehearing en banc). We consider the argument forfeited. See *Sprietsma* v. *Mercury Marine*, 537 U. S. 51, 56, n. 4 (2002).

* * *

The judgment of the Court of Appeals for the D. C. Circuit is affirmed.

It is so ordered.

SUPREME COURT OF THE UNITED STATES

No. 10–1259

UNITED STATES, PETITIONER *v.* ANTOINE JONES

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

[January 23, 2012]

JUSTICE SOTOMAYOR, concurring.

I join the Court's opinion because I agree that a search within the meaning of the Fourth Amendment occurs, at a minimum, "[w]here, as here, the Government obtains information by physically intruding on a constitutionally protected area." *Ante,* at 6, n. 3. In this case, the Government installed a Global Positioning System (GPS) tracking device on respondent Antoine Jones' Jeep without a valid warrant and without Jones' consent, then used that device to monitor the Jeep's movements over the course of four weeks. The Government usurped Jones' property for the purpose of conducting surveillance on him, thereby invading privacy interests long afforded, and undoubtedly entitled to, Fourth Amendment protection. See, *e.g., Silverman* v. *United States*, 365 U. S. 505, 511–512 (1961).

Of course, the Fourth Amendment is not concerned only with trespassory intrusions on property. See, *e.g., Kyllo* v. *United States*, 533 U. S. 27, 31–33 (2001). Rather, even in the absence of a trespass, "a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Id.*, at 33; see also *Smith* v. *Maryland*, 442 U. S. 735, 740–741 (1979); *Katz* v. *United States*, 389 U. S. 347, 361 (1967) (Harlan, J., concurring). In *Katz*, this Court enlarged its then-prevailing focus on property rights by announcing

that the reach of the Fourth Amendment does not "turn upon the presence or absence of a physical intrusion." *Id.*, at 353. As the majority's opinion makes clear, however, *Katz*'s reasonable-expectation-of-privacy test augmented, but did not displace or diminish, the common-law trespassory test that preceded it. *Ante,* at 8. Thus, "when the Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment." *United States* v. *Knotts,* 460 U. S. 276, 286 (1983) (Brennan, J., concurring in judgment); see also, *e.g.*, *Rakas* v. *Illinois,* 439 U. S. 128, 144, n. 12 (1978). JUSTICE ALITO's approach, which discounts altogether the constitutional relevance of the Government's physical intrusion on Jones' Jeep, erodes that longstanding protection for privacy expectations inherent in items of property that people possess or control. See *post,* at 5–7 (opinion concurring in judgment). By contrast, the trespassory test applied in the majority's opinion reflects an irreducible constitutional minimum: When the Government physically invades personal property to gather information, a search occurs. The reaffirmation of that principle suffices to decide this case.

Nonetheless, as JUSTICE ALITO notes, physical intrusion is now unnecessary to many forms of surveillance. *Post,* at 9–12. With increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones. See *United States* v. *Pineda-Moreno,* 617 F. 3d 1120, 1125 (CA9 2010) (Kozinski, C. J., dissenting from denial of rehearing en banc). In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance. But "[s]ituations involving merely the transmission of electronic signals without trespass

would *remain* subject to *Katz* analysis." *Ante,* at 11. As JUSTICE ALITO incisively observes, the same technological advances that have made possible nontrespassory surveillance techniques will also affect the *Katz* test by shaping the evolution of societal privacy expectations. *Post,* at 10–11. Under that rubric, I agree with JUSTICE ALITO that, at the very least, "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Post,* at 13.

In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention. 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. See, *e.g., People* v. *Weaver*, 12 N. Y. 3d 433, 441–442, 909 N. E. 2d 1195, 1199 (2009) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on"). The Government can store such records and efficiently mine them for information years into the future. *Pineda-Moreno*, 617 F. 3d, at 1124 (opinion of Kozinski, C. J.). And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility." *Illinois* v. *Lidster*, 540 U. S. 419, 426 (2004).

Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net

result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society." *United States* v. *Cuevas-Perez*, 640 F. 3d 272, 285 (CA7 2011) (Flaum, J., concurring).

I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques. See *Kyllo*, 533 U. S., at 35, n. 2; *ante*, at 11 (leaving open the possibility that duplicating traditional surveillance "through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy"). I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercises of police power to and prevent "a too permeating police surveillance," *United States* v. *Di Re*, 332 U. S. 581, 595 (1948).*

---

* *United States* v. *Knotts*, 460 U. S. 276 (1983), does not foreclose the conclusion that GPS monitoring, in the absence of a physical intrusion, is a Fourth Amendment search. As the majority's opinion notes, *Knotts* reserved the question whether "'different constitutional principles may be applicable'" to invasive law enforcement practices such as GPS tracking. See *ante*, at 8, n. 6 (quoting 460 U. S., at 284). *United States* v. *Karo*, 468 U. S. 705 (1984), addressed the Fourth

More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. *E.g., Smith*, 442 U. S., at 742; *United States* v. *Miller*, 425 U. S. 435, 443 (1976). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as JUSTICE ALITO notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," *post*, at 10, and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases

---

Amendment implications of the installation of a beeper in a container with the consent of the container's original owner, who was aware that the beeper would be used for surveillance purposes. *Id.*, at 707. Owners of GPS-equipped cars and smartphones do not contemplate that these devices will be used to enable covert surveillance of their movements. To the contrary, subscribers of one such service greeted a similar suggestion with anger. Quain, Changes to OnStar's Privacy Terms Rile Some Users, N. Y. Times (Sept. 22, 2011), online at http://wheels.blogs.nytimes.com/2011/09/22/changes-to-onstars-privacy-terms-rile-some-users (as visited Jan. 19, 2012, and available in Clerk of Court's case file). In addition, the bugged container in *Karo* lacked the close relationship with the target that a car shares with its owner. The bugged container in *Karo* was stationary for much of the Government's surveillance. See 468 U. S., at 708–710. A car's movements, by contrast, are its owner's movements.

to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection. See *Smith*, 442 U. S., at 749 (Marshall, J., dissenting) ("Privacy 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"); see also *Katz*, 389 U. S., at 351–352 ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected").

Resolution of these difficult questions in this case is unnecessary, however, because the Government's physical intrusion on Jones' Jeep supplies a narrower basis for decision. I therefore join the majority's opinion.

SUPREME COURT OF THE UNITED STATES

No. 10–1259

UNITED STATES, PETITIONER *v.* ANTOINE JONES

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE DISTRICT OF COLUMBIA CIRCUIT

[January 23, 2012]

JUSTICE ALITO, with whom JUSTICE GINSBURG, JUSTICE BREYER, and JUSTICE KAGAN join, concurring in the judgment.

This case requires us to apply the Fourth Amendment's prohibition of unreasonable searches and seizures to a 21st-century surveillance technique, the use of a Global Positioning System (GPS) device to monitor a vehicle's movements for an extended period of time. Ironically, the Court has chosen to decide this case based on 18th-century tort law. By attaching a small GPS device[1] to the underside of the vehicle that respondent drove, the law enforcement officers in this case engaged in conduct that might have provided grounds in 1791 for a suit for trespass to chattels.[2] And for this reason, the Court concludes, the installation and use of the GPS device constituted a search. *Ante*, at 3–4.

---

[1] Although the record does not reveal the size or weight of the device used in this case, there is now a device in use that weighs two ounces and is the size of a credit card. Tr. of Oral Arg. 27.

[2] At common law, a suit for trespass to chattels could be maintained if there was a violation of "the dignitary interest in the inviolability of chattels," but today there must be "some actual damage to the chattel before the action can be maintained." W. Keeton, D. Dobbs, R. Keeton, & D. Owen, Prosser & Keeton on Law of Torts 87 (5th ed. 1984) (hereinafter Prosser & Keeton). Here, there was no actual damage to the vehicle to which the GPS device was attached.

This holding, in my judgment, is unwise. It strains the language of the Fourth Amendment; it has little if any support in current Fourth Amendment case law; and it is highly artificial.

I would analyze the question presented in this case by asking whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove.

I

A

The Fourth Amendment prohibits "unreasonable searches and seizures," and the Court makes very little effort to explain how the attachment or use of the GPS device fits within these terms. The Court does not contend that there was a seizure. A seizure of property occurs when there is "some meaningful interference with an individual's possessory interests in that property," *United States* v. *Jacobsen*, 466 U. S. 109, 113 (1984), and here there was none. Indeed, the success of the surveillance technique that the officers employed was dependent on the fact that the GPS did not interfere in any way with the operation of the vehicle, for if any such interference had been detected, the device might have been discovered.

The Court does claim that the installation and use of the GPS constituted a search, see *ante*, at 3–4, but this conclusion is dependent on the questionable proposition that these two procedures cannot be separated for purposes of Fourth Amendment analysis. If these two procedures are analyzed separately, it is not at all clear from the Court's opinion why either should be regarded as a search. It is clear that the attachment of the GPS device was not itself a search; if the device had not functioned or if the officers had not used it, no information would have been obtained. And the Court does not contend that the use of the device constituted a search either. On the contrary, the Court

accepts the holding in *United States* v. *Knotts*, 460 U. S. 276 (1983), that the use of a surreptitiously planted electronic device to monitor a vehicle's movements on public roads did not amount to a search. See *ante*, at 7.

The Court argues—and I agree—that "we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" *Ante*, at 5 (quoting *Kyllo* v. *United States*, 533 U. S. 27, 34 (2001)). But it is almost impossible to think of late-18th-century situations that are analogous to what took place in this case. (Is it possible to imagine a case in which a constable secreted himself somewhere in a coach and remained there for a period of time in order to monitor the movements of the coach's owner?[3]) The Court's theory seems to be that the concept of a search, as originally understood, comprehended any technical trespass that led to the gathering of evidence, but we know that this is incorrect. At common law, any unauthorized intrusion on private property was actionable, see Prosser & Keeton 75, but a trespass on open fields, as opposed to the "curtilage" of a home, does not fall within the scope of the Fourth Amendment because private property outside the curtilage is not part of a "hous[e]" within the meaning of the Fourth Amendment. See *Oliver* v. *United States*, 466 U. S. 170 (1984); *Hester* v. *United States*, 265 U. S. 57 (1924).

B

The Court's reasoning in this case is very similar to that in the Court's early decisions involving wiretapping and electronic eavesdropping, namely, that a technical trespass followed by the gathering of evidence constitutes a

---

[3] The Court suggests that something like this might have occurred in 1791, but this would have required either a gigantic coach, a very tiny constable, or both—not to mention a constable with incredible fortitude and patience.

search. In the early electronic surveillance cases, the Court concluded that a Fourth Amendment search occurred when private conversations were monitored as a result of an "unauthorized physical penetration into the premises occupied" by the defendant. *Silverman* v. *United States*, 365 U. S. 505, 509 (1961). In *Silverman*, police officers listened to conversations in an attached home by inserting a "spike mike" through the wall that this house shared with the vacant house next door. *Id.*, at 506. This procedure was held to be a search because the mike made contact with a heating duct on the other side of the wall and thus "usurp[ed] . . . an integral part of the premises." *Id.*, at 511.

By contrast, in cases in which there was no trespass, it was held that there was no search. Thus, in *Olmstead* v. *United States*, 277 U. S. 438 (1928), the Court found that the Fourth Amendment did not apply because "[t]he taps from house lines were made in the streets near the houses." *Id.*, at 457. Similarly, the Court concluded that no search occurred in *Goldman* v. *United States*, 316 U. S. 129, 135 (1942), where a "detectaphone" was placed on the outer wall of defendant's office for the purpose of overhearing conversations held within the room.

This trespass-based rule was repeatedly criticized. In *Olmstead*, Justice Brandeis wrote that it was "immaterial where the physical connection with the telephone wires was made." 277 U. S., at 479 (dissenting opinion). Although a private conversation transmitted by wire did not fall within the literal words of the Fourth Amendment, he argued, the Amendment should be understood as prohibiting "every unjustifiable intrusion by the government upon the privacy of the individual." *Id.*, at 478. See also, *e.g.*, *Silverman*, *supra*, at 513 (Douglas, J., concurring) ("The concept of 'an unauthorized physical penetration into the premises,' on which the present decision rests seems to me beside the point. Was not the wrong . . . done when the

intimacies of the home were tapped, recorded, or revealed? The depth of the penetration of the electronic device—even the degree of its remoteness from the inside of the house—is not the measure of the injury"); *Goldman*, *supra*, at 139 (Murphy, J., dissenting) ("[T]he search of one's home or office no longer requires physical entry, for science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment").

Katz v. *United States*, 389 U. S. 347 (1967), finally did away with the old approach, holding that a trespass was not required for a Fourth Amendment violation. *Katz* involved the use of a listening device that was attached to the outside of a public telephone booth and that allowed police officers to eavesdrop on one end of the target's phone conversation. This procedure did not physically intrude on the area occupied by the target, but the *Katz* Court "repudiate[ed]" the old doctrine, *Rakas* v. *Illinois*, 439 U. S. 128, 143 (1978), and held that "[t]he fact that the electronic device employed . . . did not happen to penetrate the wall of the booth can have no constitutional significance," 389 U. S., at 353 ("[T]he reach of th[e] [Fourth] Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure"); see *Rakas*, *supra*, at 143 (describing *Katz* as holding that the "capacity to claim the protection for the Fourth Amendment depends not upon a property right in the invaded place but upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place"); *Kyllo*, *supra*, at 32 ("We have since decoupled violation of a person's Fourth Amendment rights from trespassory violation of his property"). What mattered, the Court now held, was whether the conduct at issue "violated the privacy upon which [the defendant] justifiably relied while using the telephone booth." *Katz*, *supra*,

at 353.

Under this approach, as the Court later put it when addressing the relevance of a technical trespass, "an actual trespass is neither necessary *nor sufficient* to establish a constitutional violation." *United States* v. *Karo,* 468 U. S. 705, 713 (1984) (emphasis added). *Ibid.* ("Compar[ing] *Katz* v. *United States,* 389 U. S. 347 (1967) (no trespass, but Fourth Amendment violation), with *Oliver* v. *United States,* 466 U. S. 170 (1984) (trespass, but no Fourth Amendment violation)"). In *Oliver,* the Court wrote:

> "The existence of a property right is but one element in determining whether expectations of privacy are legitimate. 'The premise that property interests control the right of the Government to search and seize has been discredited.' *Katz,* 389 U. S., at 353, (quoting *Warden* v. *Hayden,* 387 U. S. 294, 304 (1967); some internal quotation marks omitted)." 466 U. S., at 183.

II

The majority suggests that two post-*Katz* decisions—*Soldal* v. *Cook County,* 506 U. S. 56 (1992), and *Alderman* v. *United States,* 394 U. S. 165 (1969)—show that a technical trespass is sufficient to establish the existence of a search, but they provide little support.

In *Soldal,* the Court held that towing away a trailer home without the owner's consent constituted a seizure even if this did not invade the occupants' personal privacy. But in the present case, the Court does not find that there was a seizure, and it is clear that none occurred.

In *Alderman,* the Court held that the Fourth Amendment rights of homeowners were implicated by the use of a surreptitiously planted listening device to monitor third-party conversations that occurred within their home. See 394 U. S., at 176–180. *Alderman* is best understood to

mean that the homeowners had a legitimate expectation of privacy in all conversations that took place under their roof. See *Rakas*, 439 U. S., at 144, n. 12 (citing *Alderman* for the proposition that "the Court has not altogether abandoned use of property concepts in determining the presence or absence of the privacy interests protected by that Amendment"); 439 U. S., at 153 (Powell, J., concurring) (citing *Alderman* for the proposition that "property rights reflect society's explicit recognition of a person's authority to act as he wishes in certain areas, and therefore should be considered in determining whether an individual's expectations of privacy are reasonable); *Karo*, *supra*, at 732 (Stevens, J., concurring in part and dissenting in part) (citing *Alderman* in support of the proposition that "a homeowner has a reasonable expectation of privacy in the contents of his home, including items owned by others").

In sum, the majority is hard pressed to find support in post-*Katz* cases for its trespass-based theory.

III

Disharmony with a substantial body of existing case law is only one of the problems with the Court's approach in this case.

I will briefly note four others. First, the Court's reasoning largely disregards what is really important (the *use* of a GPS for the purpose of long-term tracking) and instead attaches great significance to something that most would view as relatively minor (attaching to the bottom of a car a small, light object that does not interfere in any way with the car's operation). Attaching such an object is generally regarded as so trivial that it does not provide a basis for recovery under modern tort law. See Prosser & Keeton §14, at 87 (harmless or trivial contact with personal property not actionable); D. Dobbs, Law of Torts 124 (2000) (same). But under the Court's reasoning, this conduct

may violate the Fourth Amendment. By contrast, if long-term monitoring can be accomplished without committing a technical trespass—suppose, for example, that the Federal Government required or persuaded auto manufacturers to include a GPS tracking device in every car—the Court's theory would provide no protection.

Second, the Court's approach leads to incongruous results. If the police attach a GPS device to a car and use the device to follow the car for even a brief time, under the Court's theory, the Fourth Amendment applies. But if the police follow the same car for a much longer period using unmarked cars and aerial assistance, this tracking is not subject to any Fourth Amendment constraints.

In the present case, the Fourth Amendment applies, the Court concludes, because the officers installed the GPS device after respondent's wife, to whom the car was registered, turned it over to respondent for his exclusive use. See *ante*, at 8. But if the GPS had been attached prior to that time, the Court's theory would lead to a different result. The Court proceeds on the assumption that respondent "had at least the property rights of a bailee," *ante*, at 3, n. 2, but a bailee may sue for a trespass to chattel only if the injury occurs during the term of the bailment. See 8A Am. Jur. 2d, Bailment §166, pp. 685–686 (2009). So if the GPS device had been installed before respondent's wife gave him the keys, respondent would have no claim for trespass—and, presumably, no Fourth Amendment claim either.

Third, under the Court's theory, the coverage of the Fourth Amendment may vary from State to State. If the events at issue here had occurred in a community property State[4] or a State that has adopted the Uniform Marital

[4] See, *e.g.*, Cal. Family Code Ann. §760 (West 2004).

Property Act,[5] respondent would likely be an owner of the vehicle, and it would not matter whether the GPS was installed before or after his wife turned over the keys. In non-community-property States, on the other hand, the registration of the vehicle in the name of respondent's wife would generally be regarded as presumptive evidence that she was the sole owner. See 60 C. J. S., Motor Vehicles §231, pp. 398–399 (2002); 8 Am. Jur. 2d, Automobiles §1208, pp. 859–860 (2007).

Fourth, the Court's reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked. For example, suppose that the officers in the present case had followed respondent by surreptitiously activating a stolen vehicle detection system that came with the car when it was purchased. Would the sending of a radio signal to activate this system constitute a trespass to chattels? Trespass to chattels has traditionally required a physical touching of the property. See Restatement (Second) of Torts §217 and Comment *e* (1963 and 1964); Dobbs, *supra*, at 123. In recent years, courts have wrestled with the application of this old tort in cases involving unwanted electronic contact with computer systems, and some have held that even the transmission of electrons that occurs when a communication is sent from one computer to another is enough. See, *e.g.*, *CompuServe, Inc.* v. *Cyber Promotions, Inc.* 962 F. Supp. 1015, 1021 (SD Ohio 1997); *Thrifty-Tel, Inc.* v. *Bezenek*, 46 Cal. App. 4th 1559, 1566, n. 6 (1996). But may such decisions be followed in applying the Court's trespass theory? Assuming that what matters under the Court's theory is the law of trespass as it existed at the time of the adoption of the Fourth

---

[5] See Uniform Marital Property Act §4, 9A U. L. A. 116 (1998).

Amendment, do these recent decisions represent a change in the law or simply the application of the old tort to new situations?

IV

A

The *Katz* expectation-of-privacy test avoids the problems and complications noted above, but it is not without its own difficulties. It involves a degree of circularity, see *Kyllo*, 533 U. S., at 34, and judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks. See *Minnesota* v. *Carter*, 525 U. S. 83, 97 (1998) (SCALIA, J., concurring). In addition, the *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.[6]

On the other hand, concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions. This is what ultimately happened with respect to wiretapping. After *Katz*, Congress

---

[6]See, *e.g.*, NPR, The End of Privacy http://www.npr.org/series/114250076/the-end-of-privacy (all Internet materials as visited Jan. 20, 2012, and available in Clerk of Court's case file); Time Magazine, Everything About You Is Being Tracked—Get Over It, Joel Stein, Mar. 21, 2011, Vol. 177, No. 11.

did not leave it to the courts to develop a body of Fourth Amendment case law governing that complex subject. Instead, Congress promptly enacted a comprehensive statute, see 18 U. S. C. §§2510–2522 (2006 ed. and Supp. IV), and since that time, the regulation of wiretapping has been governed primarily by statute and not by case law.[7] In an ironic sense, although *Katz* overruled *Olmstead*, Chief Justice Taft's suggestion in the latter case that the regulation of wiretapping was a matter better left for Congress, see 277 U. S., at 465–466, has been borne out.

B

Recent years have seen the emergence of many new devices that permit the monitoring of a person's movements. In some locales, closed-circuit television video monitoring is becoming ubiquitous. On toll roads, automatic toll collection systems create a precise record of the movements of motorists who choose to make use of that convenience. Many motorists purchase cars that are equipped with devices that permit a central station to ascertain the car's location at any time so that roadside assistance may be provided if needed and the car may be found if it is stolen.

Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users—and as of June 2011, it has been reported, there were more than 322 million wireless devices in use in the United States.[8] For older phones, the accuracy of the location information depends on the density of the tower network, but new "smart phones," which

---

[7] See Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 Mich. L. Rev. 801, 850–851 (2004) (hereinafter Kerr).

[8] See CTIA Consumer Info, 50 Wireless Quick Facts, http://www.ctia.org/consumer_info/index.cfm/AID/10323.

are equipped with a GPS device, permit more precise tracking. For example, when a user activates the GPS on such a phone, a provider is able to monitor the phone's location and speed of movement and can then report back real-time traffic conditions after combining ("crowdsourcing") the speed of all such phones on any particular road.[9] Similarly, phone-location-tracking services are offered as "social" tools, allowing consumers to find (or to avoid) others who enroll in these services. The availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements.

V

In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance.[10] Only an investigation of unusual importance could have justified such an

---

[9] See, *e.g.*, The bright side of sitting in traffic: Crowdsourcing road congestion data, Google Blog, http://googleblog.blogspot.com/2009/08/bright-side-of-sitting-in-traffic.html.

[10] Even with a radio transmitter like those used in *United States* v. *Knotts*, 460 U. S. 276 (1983), or *United States* v. *Karo*, 468 U. S. 705 (1984), such long-term surveillance would have been exceptionally demanding. The beepers used in those cases merely "emit[ted] periodic signals that [could] be picked up by a radio receiver." *Knotts*, 460 U.S., at 277. The signal had a limited range and could be lost if the police did not stay close enough. Indeed, in *Knotts* itself, officers lost the signal from the beeper, and only "with the assistance of a monitoring device located in a helicopter [was] the approximate location of the signal . . . picked up again about one hour later." *Id.*, at 278.

expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap. In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. See, *e.g.*, Kerr, 102 Mich. L. Rev., at 805–806. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.

To date, however, Congress and most States have not enacted statutes regulating the use of GPS tracking technology for law enforcement purposes. The best that we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated.

Under this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. See *Knotts*, 460 U. S., at 281–282. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period. In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark. Other cases may present more difficult questions. But where uncertainty exists with respect to whether a certain period of GPS surveil

lance is long enough to constitute a Fourth Amendment search, the police may always seek a warrant.[11] We also need not consider whether prolonged GPS monitoring in the context of investigations involving extraordinary offenses would similarly intrude on a constitutionally protected sphere of privacy. In such cases, long-term tracking might have been mounted using previously available techniques.

* * *

For these reasons, I conclude that the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment. I therefore agree with the majority that the decision of the Court of Appeals must be affirmed.

---

[11] In this case, the agents obtained a warrant, but they did not comply with two of the warrant's restrictions: They did not install the GPS device within the 10-day period required by the terms of the warrant and by Fed. Rule Crim. Proc. 41(e)(2)(B)(i), and they did not install the GPS device within the District of Columbia, as required by the terms of the warrant and by 18 U. S. C. §3117(a) and Rule 41(b)(4). In the courts below the Government did not argue, and has not argued here, that the Fourth Amendment does not impose these precise restrictions and that the violation of these restrictions does not demand the suppression of evidence obtained using the tracking device. See, *e.g.*, *United States* v. *Gerber*, 994 F. 2d 1556, 1559–1560 (CA11 1993); *United States* v. *Burke*, 517 F. 2d 377, 386–387 (CA2 1975). Because it was not raised, that question is not before us.

Syllabus

NOTE: Where it is feasible, a syllabus (headnote) will be released, as is being done in connection with this case, at the time the opinion is issued. The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States* v. *Detroit Timber & Lumber Co.*, 200 U. S. 321, 337.

SUPREME COURT OF THE UNITED STATES

Syllabus

CITY OF INDIANAPOLIS ET AL. *v.* EDMOND ET AL.

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

No. 99–1030. Argued October 3, 2000—Decided November 28, 2000

Petitioner city operates vehicle checkpoints on its roads in an effort to interdict unlawful drugs. Respondents, who were each stopped at such a checkpoint, filed suit, claiming that the roadblocks violated the Fourth Amendment. The District Court denied respondents a preliminary injunction, but the Seventh Circuit reversed, holding that the checkpoints contravened the Fourth Amendment.

Held: Because the checkpoint program's primary purpose is indistinguishable from the general interest in crime control, the checkpoints violate the Fourth Amendment. Pp. 3–15.

(a) The rule that a search or seizure is unreasonable under the Fourth Amendment absent individualized suspicion of wrongdoing has limited exceptions. For example, this Court has upheld brief, suspicionless seizures at a fixed checkpoint designed to intercept illegal aliens, *United States* v. *Martinez-Fuerte*, 428 U. S. 543, and at a sobriety checkpoint aimed at removing drunk drivers from the road, *Michigan Dept. of State Police* v. *Sitz*, 496 U. S. 444. The Court has also suggested that a similar roadblock to verify drivers' licenses and registrations would be permissible to serve a highway safety interest. *Delaware* v. *Prouse*, 440 U. S. 648, 663. However, the Court has never approved a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing. Pp. 3–7.

(b) The latter purpose is what principally distinguishes the checkpoints at issue from those the Court has previously approved, which were designed to serve purposes closely related to the problems of policing the border or the necessity of ensuring roadway safety. Petitioners state that the *Sitz* and *Martinez-Fuerte* checkpoints had the same ultimate purpose of arresting those suspected of committing crimes. Securing the border and apprehending drunken drivers are

Syllabus

law enforcement activities, and authorities employ arrests and criminal prosecutions to pursue these goals. But if this case were to rest at such a high level of generality, there would be little check on the authorities' ability to construct roadblocks for almost any conceivable law enforcement purpose. The checkpoint program is also not justified by the severe and intractable nature of the drug problem. The gravity of the threat alone cannot be dispositive of questions concerning what means law enforcement may employ to pursue a given purpose. Rather, in determining whether individualized suspicion is required, the Court must consider the nature of the interests threatened and their connection to the particular law enforcement practices at issue. Nor can the checkpoints' purpose be rationalized in terms of a highway safety concern similar to that in *Sitz*, or merely likened to the antismuggling purpose in *Martinez-Fuerte*. Neither *Whren* v. *United States*, 517 U. S. 806, nor *Bond* v. *United States*, 529 U. S. 334, precludes an inquiry into the checkpoint program's purposes. And if the program could be justified by its lawful secondary purposes of keeping impaired motorists off the road and verifying licenses and registrations, authorities would be able to establish checkpoints for virtually any purpose so long as they also included a license or sobriety check. That is why the Court must determine the primary purpose of the checkpoint program. This holding does not alter the constitutional status of the checkpoints approved in *Sitz* and *Martinez-Fuerte*, or the type of checkpoint suggested in *Prouse*. It also does not affect the validity of border searches or searches in airports and government buildings, where the need for such measures to ensure public safety can be particularly acute. Nor does it impair police officers' ability to act appropriately upon information that they properly learn during a checkpoint stop justified by a lawful primary purpose. Finally, the purpose inquiry is to be conducted only at the programmatic level and is not an invitation to probe the minds of individual officers acting at the scene. Pp. 7–15.

183 F. 3d 659, affirmed.

O'CONNOR, J., delivered the opinion of the Court, in which STEVENS, KENNEDY, SOUTER, GINSBURG, and BREYER, JJ., joined. REHNQUIST, C. J., filed a dissenting opinion, in which THOMAS, J., joined, and in which SCALIA, J., joined as to Part I. THOMAS, J., filed a dissenting opinion.

SUPREME COURT OF THE UNITED STATES

No. 99–1030

CITY OF INDIANAPOLIS, ET AL., PETITIONERS *v.* JAMES EDMOND ET AL.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SEVENTH CIRCUIT

[November 28, 2000]

JUSTICE O'CONNOR delivered the opinion of the Court.

In *Michigan Dept. of State Police* v. *Sitz,* 496 U. S. 444 (1990), and *United States* v. *Martinez-Fuerte,* 428 U. S. 543 (1976), we held that brief, suspicionless seizures at highway checkpoints for the purposes of combating drunk driving and intercepting illegal immigrants were constitutional. We now consider the constitutionality of a highway checkpoint program whose primary purpose is the discovery and interdiction of illegal narcotics.

I

In August 1998, the city of Indianapolis began to operate vehicle checkpoints on Indianapolis roads in an effort to interdict unlawful drugs. The city conducted six such roadblocks between August and November that year, stopping 1,161 vehicles and arresting 104 motorists. Fifty-five arrests were for drug-related crimes, while 49 were for offenses unrelated to drugs. *Edmond* v. *Goldsmith,* 183 F. 3d 659, 661 (CA7 1999). The overall "hit rate" of the program was thus approximately nine percent.

The parties stipulated to the facts concerning the operation of the checkpoints by the Indianapolis Police Depart-

ment (IPD) for purposes of the preliminary injunction proceedings instituted below. At each checkpoint location, the police stop a predetermined number of vehicles. Approximately 30 officers are stationed at the checkpoint. Pursuant to written directives issued by the chief of police, at least one officer approaches the vehicle, advises the driver that he or she is being stopped briefly at a drug checkpoint, and asks the driver to produce a license and registration. The officer also looks for signs of impairment and conducts an open-view examination of the vehicle from the outside. A narcotics-detection dog walks around the outside of each stopped vehicle.

The directives instruct the officers that they may conduct a search only by consent or based on the appropriate quantum of particularized suspicion. The officers must conduct each stop in the same manner until particularized suspicion develops, and the officers have no discretion to stop any vehicle out of sequence. The city agreed in the stipulation to operate the checkpoints in such a way as to ensure that the total duration of each stop, absent reasonable suspicion or probable cause, would be five minutes or less.

The affidavit of Indianapolis Police Sergeant Marshall DePew, although it is technically outside the parties' stipulation, provides further insight concerning the operation of the checkpoints. According to Sergeant DePew, checkpoint locations are selected weeks in advance based on such considerations as area crime statistics and traffic flow. The checkpoints are generally operated during daylight hours and are identified with lighted signs reading, "NARCOTICS CHECKPOINT ___ MILE AHEAD, NARCOTICS K–9 IN USE, BE PREPARED TO STOP." App. to Pet. for Cert. 57a. Once a group of cars has been stopped, other traffic proceeds without interruption until all the stopped cars have been processed or diverted for further processing. Sergeant DePew also stated that the

average stop for a vehicle not subject to further processing lasts two to three minutes or less.

Respondents James Edmond and Joell Palmer were each stopped at a narcotics checkpoint in late September 1998. Respondents then filed a lawsuit on behalf of themselves and the class of all motorists who had been stopped or were subject to being stopped in the future at the Indianapolis drug checkpoints. Respondents claimed that the roadblocks violated the Fourth Amendment of the United States Constitution and the search and seizure provision of the Indiana Constitution. Respondents requested declaratory and injunctive relief for the class, as well as damages and attorney's fees for themselves.

Respondents then moved for a preliminary injunction. Although respondents alleged that the officers who stopped them did not follow the written directives, they agreed to the stipulation concerning the operation of the checkpoints for purposes of the preliminary injunction proceedings. The parties also stipulated to certification of the plaintiff class. The United States District Court for the Southern District of Indiana agreed to class certification and denied the motion for a preliminary injunction, holding that the checkpoint program did not violate the Fourth Amendment. *Edmond* v. *Goldsmith,* 38 F. Supp. 2d 1016 (1998). A divided panel of the United States Court of Appeals for the Seventh Circuit reversed, holding that the checkpoints contravened the Fourth Amendment. 183 F. 3d 659 (1999). The panel denied rehearing. We granted certiorari, 528 U. S. 1153 (2000), and now affirm.

II

The Fourth Amendment requires that searches and seizures be reasonable. A search or seizure is ordinarily unreasonable in the absence of individualized suspicion of wrongdoing. *Chandler* v. *Miller,* 520 U. S. 305, 308 (1997). While such suspicion is not an "irreducible" component of

reasonableness, *Martinez-Fuerte,* 428 U. S., at 561, we have recognized only limited circumstances in which the usual rule does not apply. For example, we have upheld certain regimes of suspicionless searches where the program was designed to serve "special needs, beyond the normal need for law enforcement." See, *e.g., Vernonia School Dist. 47J* v. *Acton,* 515 U. S. 646 (1995) (random drug testing of student-athletes); *Treasury Employees* v. *Von Raab,* 489 U. S. 656 (1989) (drug tests for United States Customs Service employees seeking transfer or promotion to certain positions); *Skinner* v. *Railway Labor Executives' Assn.,* 489 U. S. 602 (1989) (drug and alcohol tests for railway employees involved in train accidents or found to be in violation of particular safety regulations). We have also allowed searches for certain administrative purposes without particularized suspicion of misconduct, provided that those searches are appropriately limited. See, *e.g., New York* v. *Burger,* 482 U. S. 691, 702–704 (1987) (warrantless administrative inspection of premises of "closely regulated" business); *Michigan* v. *Tyler,* 436 U. S. 499, 507–509, 511–512 (1978) (administrative inspection of fire-damaged premises to determine cause of blaze); *Camara* v. *Municipal Court of City and County of San Francisco,* 387 U. S. 523, 534–539 (1967) (administrative inspection to ensure compliance with city housing code).

We have also upheld brief, suspicionless seizures of motorists at a fixed Border Patrol checkpoint designed to intercept illegal aliens, *Martinez-Fuerte, supra,* and at a sobriety checkpoint aimed at removing drunk drivers from the road, *Michigan Dept. of State Police* v. *Sitz,* 496 U. S. 444 (1990). In addition, in *Delaware* v. *Prouse,* 440 U. S. 648, 663 (1979), we suggested that a similar type of roadblock with the purpose of verifying drivers' licenses and vehicle registrations would be permissible. In none of these cases, however, did we indicate approval of a check-

point program whose primary purpose was to detect evidence of ordinary criminal wrongdoing.

In *Martinez-Fuerte,* we entertained Fourth Amendment challenges to stops at two permanent immigration checkpoints located on major United States highways less than 100 miles from the Mexican border. We noted at the outset the particular context in which the constitutional question arose, describing in some detail the "formidable law enforcement problems" posed by the northbound tide of illegal entrants into the United States. *Martinez-Fuerte, supra,* at 551–554. These problems had also been the focus of several earlier cases addressing the constitutionality of other Border Patrol traffic-checking operations. See *United States* v. *Ortiz,* 422 U. S. 891 (1975); *United States* v. *Brignoni-Ponce,* 422 U. S. 873 (1975); *Almeida-Sanchez* v. *United States,* 413 U. S. 266 (1973). In *Martinez-Fuerte,* we found that the balance tipped in favor of the Government's interests in policing the Nation's borders. 428 U. S., at 561–564. In so finding, we emphasized the difficulty of effectively containing illegal immigration at the border itself. *Id.,* at 556. We also stressed the impracticality of the particularized study of a given car to discern whether it was transporting illegal aliens, as well as the relatively modest degree of intrusion entailed by the stops. *Id.,* at 556–564.

Our subsequent cases have confirmed that considerations specifically related to the need to police the border were a significant factor in our *Martinez-Fuerte* decision. For example, in *United States* v. *Montoya de Hernandez,* 473 U. S. 531, 538 (1985), we counted *Martinez-Fuerte* as one of a number of Fourth Amendment cases that "reflect longstanding concern for the protection of the integrity of the border." Although the stops in *Martinez-Fuerte* did not occur at the border itself, the checkpoints were located near the border and served a border control function made necessary by the difficulty of guarding the border's entire

length. See *Martinez-Fuerte, supra,* at 556.

In *Sitz,* we evaluated the constitutionality of a Michigan highway sobriety checkpoint program. The *Sitz* checkpoint involved brief suspicionless stops of motorists so that police officers could detect signs of intoxication and remove impaired drivers from the road. 496 U. S., at 447–448. Motorists who exhibited signs of intoxication were diverted for a license and registration check and, if warranted, further sobriety tests. *Id.,* at 447. This checkpoint program was clearly aimed at reducing the immediate hazard posed by the presence of drunk drivers on the highways, and there was an obvious connection between the imperative of highway safety and the law enforcement practice at issue. The gravity of the drunk driving problem and the magnitude of the State's interest in getting drunk drivers off the road weighed heavily in our determination that the program was constitutional. See *id.,* at 451.

In *Prouse,* we invalidated a discretionary, suspicionless stop for a spot check of a motorist's driver's license and vehicle registration. The officer's conduct in that case was unconstitutional primarily on account of his exercise of "standardless and unconstrained discretion." 440 U. S., at 661. We nonetheless acknowledged the States' "vital interest in ensuring that only those qualified to do so are permitted to operate motor vehicles, that these vehicles are fit for safe operation, and hence that licensing, registration, and vehicle inspection requirements are being observed." *Id.,* at 658. Accordingly, we suggested that "[q]uestioning of all oncoming traffic at roadblock-type stops" would be a lawful means of serving this interest in highway safety. *Id.,* at 663.

We further indicated in *Prouse* that we considered the purposes of such a hypothetical roadblock to be distinct from a general purpose of investigating crime. The State proffered the additional interests of "the apprehension of

stolen motor vehicles and of drivers under the influence of alcohol or narcotics" in its effort to justify the discretionary spot check. *Id.*, at 659, n. 18. We attributed the entirety of the latter interest to the State's interest in roadway safety. *Ibid.* We also noted that the interest in apprehending stolen vehicles may be partly subsumed by the interest in roadway safety. *Ibid.* We observed, however, that "[t]he remaining governmental interest in controlling automobile thefts is not distinguishable from the general interest in crime control." *Ibid.* Not only does the common thread of highway safety thus run through *Sitz* and *Prouse*, but *Prouse* itself reveals a difference in the Fourth Amendment significance of highway safety interests and the general interest in crime control.

III

It is well established that a vehicle stop at a highway checkpoint effectuates a seizure within the meaning of the Fourth Amendment. See, *e.g.*, *Sitz*, *supra*, at 450. The fact that officers walk a narcotics-detection dog around the exterior of each car at the Indianapolis checkpoints does not transform the seizure into a search. See *United States* v. *Place*, 462 U. S. 696, 707 (1983). Just as in *Place*, an exterior sniff of an automobile does not require entry into the car and is not designed to disclose any information other than the presence or absence of narcotics. See *ibid.* Like the dog sniff in *Place*, a sniff by a dog that simply walks around a car is "much less intrusive than a typical search." *Ibid.* Cf. *United States* v. *Turpin*, 920 F. 2d 1377, 1385 (CA8 1990). Rather, what principally distinguishes these checkpoints from those we have previously approved is their primary purpose.

As petitioners concede, the Indianapolis checkpoint program unquestionably has the primary purpose of interdicting illegal narcotics. In their stipulation of facts, the parties repeatedly refer to the checkpoints as "drug

checkpoints" and describe them as "being operated by the City of Indianapolis in an effort to interdict unlawful drugs in Indianapolis." App. to Pet. for Cert. 51a–52a. In addition, the first document attached to the parties' stipulation is entitled "DRUG CHECKPOINT CONTACT OFFICER DIRECTIVES BY ORDER OF THE CHIEF OF POLICE." *Id.*, at 53a. These directives instruct officers to "[a]dvise the citizen that they are being stopped briefly at a drug checkpoint." *Ibid.* The second document attached to the stipulation is entitled "1998 Drug Road Blocks" and contains a statistical breakdown of information relating to the checkpoints conducted. *Id.*, at 55a. Further, according to Sergeant DePew, the checkpoints are identified with lighted signs reading, "NARCOTICS CHECKPOINT ___ MILE AHEAD, NARCOTICS K–9 IN USE, BE PREPARED TO STOP." *Id.*, at 57a. Finally, both the District Court and the Court of Appeals recognized that the primary purpose of the roadblocks is the interdiction of narcotics. 38 F. Supp. 2d, at 1026 (noting that both parties "stress the primary purpose of the roadblocks as the interdiction of narcotics" and that "[t]he IPD has made it clear that the purpose for its checkpoints is to interdict narcotics traffic"); 183 F. 3d, at 665 (observing that "the City concedes that its proximate goal is to catch drug offenders").

We have never approved a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing. Rather, our checkpoint cases have recognized only limited exceptions to the general rule that a seizure must be accompanied by some measure of individualized suspicion. We suggested in *Prouse* that we would not credit the "general interest in crime control" as justification for a regime of suspicionless stops. 440 U. S., at 659, n. 18. Consistent with this suggestion, each of the checkpoint programs that we have approved was designed primarily to serve purposes closely related to the problems

of policing the border or the necessity of ensuring roadway safety. Because the primary purpose of the Indianapolis narcotics checkpoint program is to uncover evidence of ordinary criminal wrongdoing, the program contravenes the Fourth Amendment.

Petitioners propose several ways in which the narcotics-detection purpose of the instant checkpoint program may instead resemble the primary purposes of the checkpoints in *Sitz* and *Martinez-Fuerte*. Petitioners state that the checkpoints in those cases had the same ultimate purpose of arresting those suspected of committing crimes. Brief for Petitioners 22. Securing the border and apprehending drunk drivers are, of course, law enforcement activities, and law enforcement officers employ arrests and criminal prosecutions in pursuit of these goals. See *Sitz*, 496 U. S., at 447, 450; *Martinez-Fuerte*, 428 U. S., at 545–550. If we were to rest the case at this high level of generality, there would be little check on the ability of the authorities to construct roadblocks for almost any conceivable law enforcement purpose. Without drawing the line at roadblocks designed primarily to serve the general interest in crime control, the Fourth Amendment would do little to prevent such intrusions from becoming a routine part of American life.

Petitioners also emphasize the severe and intractable nature of the drug problem as justification for the checkpoint program. Brief for Petitioners 14–17, 31. There is no doubt that traffic in illegal narcotics creates social harms of the first magnitude. Cf. *Von Raab*, 489 U. S., at 668. The law enforcement problems that the drug trade creates likewise remain daunting and complex, particularly in light of the myriad forms of spin-off crime that it spawns. Cf. *Montoya de Hernandez*, 473 U. S., at 538. The same can be said of various other illegal activities, if only to a lesser degree. But the gravity of the threat alone cannot be dispositive of questions concerning what means

law enforcement officers may employ to pursue a given purpose. Rather, in determining whether individualized suspicion is required, we must consider the nature of the interests threatened and their connection to the particular law enforcement practices at issue. We are particularly reluctant to recognize exceptions to the general rule of individualized suspicion where governmental authorities primarily pursue their general crime control ends.

Nor can the narcotics-interdiction purpose of the checkpoints be rationalized in terms of a highway safety concern similar to that present in *Sitz*. The detection and punishment of almost any criminal offense serves broadly the safety of the community, and our streets would no doubt be safer but for the scourge of illegal drugs. Only with respect to a smaller class of offenses, however, is society confronted with the type of immediate, vehicle-bound threat to life and limb that the sobriety checkpoint in *Sitz* was designed to eliminate.

Petitioners also liken the anticontraband agenda of the Indianapolis checkpoints to the antismuggling purpose of the checkpoints in *Martinez-Fuerte*. Brief for Petitioners 15–16. Petitioners cite this Court's conclusion in *Martinez-Fuerte* that the flow of traffic was too heavy to permit "particularized study of a given car that would enable it to be identified as a possible carrier of illegal aliens," *Martinez-Fuerte, supra,* at 557, and claim that this logic has even more force here. The problem with this argument is that the same logic prevails any time a vehicle is employed to conceal contraband or other evidence of a crime. This type of connection to the roadway is very different from the close connection to roadway safety that was present in *Sitz* and *Prouse*. Further, the Indianapolis checkpoints are far removed from the border context that was crucial in *Martinez-Fuerte*. While the difficulty of examining each passing car was an important factor in validating the law enforcement technique employed in

Martinez-Fuerte, this factor alone cannot justify a regime of suspicionless searches or seizures. Rather, we must look more closely at the nature of the public interests that such a regime is designed principally to serve.

The primary purpose of the Indianapolis narcotics checkpoints is in the end to advance "the general interest in crime control," *Prouse,* 440 U. S., at 659, n. 18. We decline to suspend the usual requirement of individualized suspicion where the police seek to employ a checkpoint primarily for the ordinary enterprise of investigating crimes. We cannot sanction stops justified only by the generalized and ever-present possibility that interrogation and inspection may reveal that any given motorist has committed some crime.

Of course, there are circumstances that may justify a law enforcement checkpoint where the primary purpose would otherwise, but for some emergency, relate to ordinary crime control. For example, as the Court of Appeals noted, the Fourth Amendment would almost certainly permit an appropriately tailored roadblock set up to thwart an imminent terrorist attack or to catch a dangerous criminal who is likely to flee by way of a particular route. See 183 F. 3d, at 662–663. The exigencies created by these scenarios are far removed from the circumstances under which authorities might simply stop cars as a matter of course to see if there just happens to be a felon leaving the jurisdiction. While we do not limit the purposes that may justify a checkpoint program to any rigid set of categories, we decline to approve a program whose primary purpose is ultimately indistinguishable from the general interest in crime control.[1]

---

[1]THE CHIEF JUSTICE'S dissent erroneously characterizes our opinion as resting on the application of a "non-law-enforcement primary purpose test." *Post,* at 6. Our opinion nowhere describes the purposes of the *Sitz* and *Martinez-Fuerte* checkpoints as being "not primarily

Petitioners argue that our prior cases preclude an inquiry into the purposes of the checkpoint program. For example, they cite *Whren* v. *United States,* 517 U. S. 806 (1996), and *Bond* v. *United States,* 529 U. S. 334 (2000), to support the proposition that "where the government articulates and pursues a legitimate interest for a suspicionless stop, courts should not look behind that interest to determine whether the government's 'primary purpose' is valid." Brief for Petitioners 34; see also *id.,* at 9. These cases, however, do not control the instant situation.

In *Whren,* we held that an individual officer's subjective intentions are irrelevant to the Fourth Amendment validity of a traffic stop that is justified objectively by probable cause to believe that a traffic violation has occurred. 517 U. S., at 810–813. We observed that our prior cases "foreclose any argument that the constitutional reasonableness of traffic stops depends on the actual motivations of the individual officers involved." *Id.,* at 813. In so holding, we expressly distinguished cases where we had addressed the validity of searches conducted in the absence of probable cause. See *id.,* at 811–812 (distinguishing *Florida* v. *Wells,* 495 U. S. 1, 4 (1990) (stating that "an inventory search must not be a ruse for a general rummaging in order to discover incriminating evidence"), *Colorado* v. *Bertine,* 479 U. S. 367, 372 (1987) (suggesting that the absence of bad faith and the lack of a purely investigative purpose were relevant to the validity of an inventory

---

related to criminal law enforcement." *Post,* at 3. Rather, our judgment turns on the fact that the primary purpose of the Indianapolis checkpoints is to advance the general interest in crime control.

THE CHIEF JUSTICE'S dissent also erroneously characterizes our opinion as holding that the "use of a drug-sniffing dog . . . annuls what is otherwise plainly constitutional under our Fourth Amendment jurisprudence." *Post,* at 1. Again, the constitutional defect of the program is that its primary purpose is to advance the general interest in crime control.

search), and *Burger,* 482 U. S., at 716–717, n. 27 (observing that a valid administrative inspection conducted with neither a warrant nor probable cause did not appear to be a pretext for gathering evidence of violations of the penal laws)).

Whren therefore reinforces the principle that, while "[s]ubjective intentions play no role in ordinary, probable-cause Fourth Amendment analysis," 517 U. S., at 813, programmatic purposes may be relevant to the validity of Fourth Amendment intrusions undertaken pursuant to a general scheme without individualized suspicion. Accordingly, *Whren* does not preclude an inquiry into programmatic purpose in such contexts. Cf. *Chandler* v. *Miller,* 520 U. S. 305 (1997); *Treasury Employees* v. *Von Raab,* 489 U. S. 656 (1989); *Burger, supra*; *Michigan* v. *Tyler,* 436 U. S. 499 (1978); *Camara* v. *Municipal Court of City and County of San Francisco,* 387 U. S. 523 (1967). It likewise does not preclude an inquiry into programmatic purpose here.

Last Term in *Bond,* we addressed the question whether a law enforcement officer violated a reasonable expectation of privacy in conducting a tactile examination of carry-on luggage in the overhead compartment of a bus. In doing so, we simply noted that the principle of *Whren* rendered the subjective intent of an officer irrelevant to this analysis. 529 U. S., at 338, n. 2. While, as petitioners correctly observe, the analytical rubric of *Bond* was not "ordinary, probable-cause Fourth Amendment analysis," *Whren, supra,* at 813, nothing in *Bond* suggests that we would extend the principle of *Whren* to all situations where individualized suspicion was lacking. Rather, subjective intent was irrelevant in *Bond* because the inquiry that our precedents required focused on the objective effects of the actions of an individual officer. By contrast, our cases dealing with intrusions that occur pursuant to a general scheme absent individualized suspicion

have often required an inquiry into purpose at the programmatic level.

Petitioners argue that the Indianapolis checkpoint program is justified by its lawful secondary purposes of keeping impaired motorists off the road and verifying licenses and registrations. Brief for Petitioners 31–34. If this were the case, however, law enforcement authorities would be able to establish checkpoints for virtually any purpose so long as they also included a license or sobriety check. For this reason, we examine the available evidence to determine the primary purpose of the checkpoint program. While we recognize the challenges inherent in a purpose inquiry, courts routinely engage in this enterprise in many areas of constitutional jurisprudence as a means of sifting abusive governmental conduct from that which is lawful. Cf. 183 F. 3d, at 665. As a result, a program driven by an impermissible purpose may be proscribed while a program impelled by licit purposes is permitted, even though the challenged conduct may be outwardly similar. While reasonableness under the Fourth Amendment is predominantly an objective inquiry, our special needs and administrative search cases demonstrate that purpose is often relevant when suspicionless intrusions pursuant to a general scheme are at issue.[2]

It goes without saying that our holding today does

---

[2] Because petitioners concede that the primary purpose of the Indianapolis checkpoints is narcotics detection, we need not decide whether the State may establish a checkpoint program with the primary purpose of checking licenses or driver sobriety and a secondary purpose of interdicting narcotics. Specifically, we express no view on the question whether police may expand the scope of a license or sobriety checkpoint seizure in order to detect the presence of drugs in a stopped car. Cf. *New Jersey* v. *T. L. O.*, 469 U. S. 325, 341 (1985) (search must be "'reasonably related in scope to the circumstance which justified the interference in the first place'" (quoting *Terry* v. *Ohio*, 392 U. S. 1, 20 (1968))); *Michigan* v. *Clifford*, 464 U. S. 287, 294–295 (1984) (plurality opinion).

nothing to alter the constitutional status of the sobriety and border checkpoints that we approved in *Sitz* and *Martinez-Fuerte*, or of the type of traffic checkpoint that we suggested would be lawful in *Prouse*. The constitutionality of such checkpoint programs still depends on a balancing of the competing interests at stake and the effectiveness of the program. See *Sitz*, 496 U. S., at 450–455; *Martinez-Fuerte*, 428 U. S., at 556–564. When law enforcement authorities pursue primarily general crime control purposes at checkpoints such as here, however, stops can only be justified by some quantum of individualized suspicion.

Our holding also does not affect the validity of border searches or searches at places like airports and government buildings, where the need for such measures to ensure public safety can be particularly acute. Nor does our opinion speak to other intrusions aimed primarily at purposes beyond the general interest in crime control. Our holding also does not impair the ability of police officers to act appropriately upon information that they properly learn during a checkpoint stop justified by a lawful primary purpose, even where such action may result in the arrest of a motorist for an offense unrelated to that purpose. Finally, we caution that the purpose inquiry in this context is to be conducted only at the programmatic level and is not an invitation to probe the minds of individual officers acting at the scene. Cf. *Whren, supra*.

Because the primary purpose of the Indianapolis checkpoint program is ultimately indistinguishable from the general interest in crime control, the checkpoints violate the Fourth Amendment. The judgment of the Court of Appeals is accordingly affirmed.

It is so ordered.

SUPREME COURT OF THE UNITED STATES

No. 99–1030

CITY OF INDIANAPOLIS, ET AL., PETITIONERS *v.* JAMES EDMOND ET AL.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SEVENTH CIRCUIT

[November 28, 2000]

CHIEF JUSTICE REHNQUIST, with whom JUSTICE THOMAS joins, and with whom JUSTICE SCALIA joins as to Part I, dissenting.

The State's use of a drug-sniffing dog, according to the Court's holding, annuls what is otherwise plainly constitutional under our Fourth Amendment jurisprudence: brief, standardized, discretionless, roadblock seizures of automobiles, seizures which effectively serve a weighty state interest with only minimal intrusion on the privacy of their occupants. Because these seizures serve the State's accepted and significant interests of preventing drunken driving and checking for driver's licenses and vehicle registrations, and because there is nothing in the record to indicate that the addition of the dog sniff lengthens these otherwise legitimate seizures, I dissent.

I

As it is nowhere to be found in the Court's opinion, I begin with blackletter roadblock seizure law. "The principal protection of Fourth Amendment rights at checkpoints lies in appropriate limitations on the scope of the stop." *United States* v. *Martinez-Fuerte*, 428 U. S. 543, 566–567 (1976). Roadblock seizures are consistent with the Fourth Amendment if they are "carried out pursuant to a plan embodying explicit, neutral limitations on the conduct of

individual officers." *Brown* v. *Texas*, 443 U. S. 47, 51 (1979). Specifically, the constitutionality of a seizure turns upon "a weighing of the gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual liberty." *Id.*, at 50–51.

We first applied these principles in *Martinez-Fuerte*, *supra*, which approved highway checkpoints for detecting illegal aliens. In *Martinez-Fuerte*, we balanced the United States' formidable interest in checking the flow of illegal immigrants against the limited "objective" and "subjective" intrusion on the motorists. The objective intrusion—the stop itself,[1] the brief questioning of the occupants, and the visual inspection of the car—was considered "limited" because "[n]either the vehicle nor its occupants [were] searched." *Id.*, at 558. Likewise, the subjective intrusion, or the fear and surprise engendered in law-abiding motorists by the nature of the stop, was found to be minimal because the "regularized manner in which [the] established checkpoints [were] operated [was] visible evidence, reassuring to law-abiding motorists, that the stops [were] duly authorized and believed to serve the public interest." *Id.*, at 559. Indeed, the standardized operation of the roadblocks was viewed as markedly different from roving patrols, where the unbridled discretion of officers in the field could result in unlimited interference with motorists' use of the highways. Cf. *United States* v. *Brignoni-Ponce*, 422 U. S. 873 (1975). And although the decision in *Martinez-Fuerte* did not turn on the checkpoints' effectiveness, the record in one of the consolidated cases demonstrated that illegal aliens were found in 0.12 percent of the

[1]The record from one of the consolidated cases indicated that the stops lasted between three and five minutes. See *United States* v. *Martinez-Fuerte*, 428 U. S. 543, 546–547 (1976).

stopped vehicles. See 428 U. S., at 554.

In *Michigan Dept. of State Police* v. *Sitz*, 496 U. S. 444 (1990), we upheld the State's use of a highway sobriety checkpoint after applying the framework set out in *Martinez-Fuerte*, *supra*, and *Brown* v. *Texas*, *supra*. There, we recognized the gravity of the State's interest in curbing drunken driving and found the objective intrusion of the approximately 25-second seizure to be "slight." 496 U. S., at 451. Turning to the subjective intrusion, we noted that the checkpoint was selected pursuant to guidelines and was operated by uniformed officers. See *id.*, at 453. Finally, we concluded that the program effectively furthered the State's interest because the checkpoint resulted in the arrest of two drunk drivers, or 1.6 percent of the 126 drivers stopped. See *id.*, at 455–456.

This case follows naturally from *Martinez-Fuerte* and *Sitz*. Petitioners acknowledge that the "primary purpose" of these roadblocks is to interdict illegal drugs, but this fact should not be controlling. Even accepting the Court's conclusion that the checkpoints at issue in *Martinez-Fuerte* and *Sitz* were not primarily related to criminal law enforcement,[2] the question whether a law enforcement purpose could support a roadblock seizure is not presented in this case. The District Court found that another "purpose of the checkpoints is to check driver's licenses and vehicle registrations," App. to Pet. for Cert. 44a, and the

---

[2]This gloss, see *ante*, at 5–7, 8–10, is not at all obvious. The respondents in *Martinez-Fuerte* were criminally prosecuted for illegally transporting aliens, and the Court expressly noted that "[i]nterdicting the flow of illegal entrants from Mexico poses formidable law enforcement problems." 428 U. S., at 552. And the *Sitz* Court recognized that if an "officer's observations suggest that the driver was intoxicated, an arrest would be made." *Michigan Dept. of State Police* v. *Sitz*, 496 U. S. 444, 447 (1990). But however persuasive the distinction, the Court's opinion does not impugn the continuing validity of *Martinez-Fuerte* and *Sitz*. See *ante*, at 14–15.

written directives state that the police officers are to "[l]ook for signs of impairment." *Id.*, at 53a. The use of roadblocks to look for signs of impairment was validated by *Sitz*, and the use of roadblocks to check for driver's licenses and vehicle registrations was expressly recognized in *Delaware* v. *Prouse*, 440 U. S. 648, 663 (1979).[3] That the roadblocks serve these legitimate state interests cannot be seriously disputed, as the 49 people arrested for offenses unrelated to drugs can attest. *Edmond* v. *Goldsmith*, 183 F. 3d 659, 661 (CA7 1999). And it would be speculative to conclude—given the District Court's findings, the written directives, and the actual arrests—that petitioners would not have operated these roadblocks but for the State's interest in interdicting drugs.

Because of the valid reasons for conducting these roadblock seizures, it is constitutionally irrelevant that petitioners also hoped to interdict drugs. In *Whren* v. *United States*, 517 U. S. 806 (1996), we held that an officer's subjective intent would not invalidate an otherwise objectively justifiable stop of an automobile. The reasonableness of an officer's discretionary decision to stop an automobile, at issue in *Whren*, turns on whether there is probable cause to believe that a traffic violation has occurred. The reasonableness of highway checkpoints, at issue here, turns on whether they effectively serve a significant state interest with minimal intrusion on motorists. The stop in *Whren* was objectively reasonable because the police officers had witnessed traffic violations; so too the roadblocks here are objectively reasonable because they serve the substantial interests of preventing drunken driving and checking for driver's licenses and vehicle

---

[3] Several Courts of Appeals have upheld roadblocks that check for driver's licenses and vehicle registrations. See, *e.g.*, *United States* v. *Galindo-Gonzales*, 142 F. 3d 1217 (CA10 1998); *United States* v. *McFayden*, 865 F. 2d 1306 (CADC 1989).

registrations with minimal intrusion on motorists.

Once the constitutional requirements for a particular seizure are satisfied, the subjective expectations of those responsible for it, be it police officers or members of a city council, are irrelevant. Cf. *Scott* v. *United States*, 436 U. S. 128, 136 (1978) ("Subjective intent alone . . . does not make otherwise lawful conduct illegal or unconstitutional"). It is the objective effect of the State's actions on the privacy of the individual that animates the Fourth Amendment. See *Bond* v. *United States*, 529 U. S. 334, 338, n. 2 (2000) (applying *Whren* to determine if an officer's conduct amounted to a "search" under the Fourth Amendment because "the issue is not his state of mind, but the objective effect of his actions"). Because the objective intrusion of a valid seizure does not turn upon anyone's subjective thoughts, neither should our constitutional analysis.[4]

With these checkpoints serving two important state interests, the remaining prongs of the *Brown* v. *Texas* balancing test are easily met. The seizure is objectively reasonable as it lasts, on average, two to three minutes and does not involve a search. App. to Pet. for Cert. 57a. The subjective intrusion is likewise limited as the checkpoints are clearly marked and operated by uniformed officers who are directed to stop every vehicle in the same manner. *Ibid.* The only difference between this case and *Sitz* is the presence of the dog. We have already held, however, that a "sniff test" by a trained narcotics dog is not a "search" within the meaning of the Fourth Amendment because it does not require physical intrusion of the object being sniffed and it does not expose anything other

---

[4] Of course we have looked to the purpose of the program in analyzing the constitutionality of certain suspicionless searches. As discussed in Part II, *infra*, that doctrine has never been applied to seizures of automobiles.

than the contraband items. *United States* v. *Place*, 462 U. S. 696, 706–707 (1983). And there is nothing in the record to indicate that the dog sniff lengthens the stop. Finally, the checkpoints' success rate—49 arrests for offenses unrelated to drugs—only confirms the State's legitimate interests in preventing drunken driving and ensuring the proper licensing of drivers and registration of their vehicles. 183 F. 3d, at 661.[5]

These stops effectively serve the State's legitimate interests; they are executed in a regularized and neutral manner; and they only minimally intrude upon the privacy of the motorists. They should therefore be constitutional.

II

The Court, unwilling to adopt the straightforward analysis that these precedents dictate, adds a new non-law-enforcement primary purpose test lifted from a distinct area of Fourth Amendment jurisprudence relating to the *searches* of homes and businesses. As discussed above, the question that the Court answers is not even posed in this case given the accepted reasons for the seizures. But more fundamentally, whatever sense a non-law-enforcement primary purpose test may make in the search setting, it is ill suited to brief roadblock seizures, where we have consistently looked at "the scope of the stop" in assessing a program's constitutionality. *Martinez-Fuerte*, 428 U. S., at 567.

We have already rejected an invitation to apply the non-law-enforcement primary purpose test that the Court now finds so indispensable. The respondents in *Sitz* argued that the *Brown* v. *Texas* balancing test was not the "proper method of analysis" with regards to roadblock seizures:

---

[5]Put in statistical terms, 4.2 percent of the 1,161 motorists stopped were arrested for offenses unrelated to drugs.

> "Respondents argue that there must be a showing of some special governmental need 'beyond the normal need' for criminal law enforcement before a balancing analysis is appropriate, and that [the State] ha[s] demonstrated no such special need.
>
> "But it is perfectly plain from a reading of [*Treasury Employees* v.] *Von Raab*[, 489 U. S. 656 (1989)], which cited and discussed with approval our earlier decision in *United States* v. *Martinez-Fuerte*, 428 U. S. 543 (1976), that it was in no way designed to repudiate our prior cases dealing with police stops of motorists on public highways. *Martinez-Fuerte*, *supra*, which utilized a balancing analysis in approving highway checkpoints for detecting illegal aliens, and *Brown* v. *Texas*, *supra*, are the relevant authorities here." 496 U. S., at 449, 450.

Considerations of *stare decisis* aside, the "perfectly plain" reason for not incorporating the "special needs" test in our roadblock seizure cases is that seizures of automobiles "deal neither with searches nor with the sanctity of private dwellings, ordinarily afforded the most stringent Fourth Amendment protection." *Martinez-Fuerte*, *supra*, at 561.

The "special needs" doctrine, which has been used to uphold certain suspicionless searches performed for reasons unrelated to law enforcement, is an exception to the general rule that a search must be based on individualized suspicion of wrongdoing. See, *e.g.*, *Skinner* v. *Railway Labor Executives' Assn.*, 489 U. S. 602 (1989) (drug test search); *Camara* v. *Municipal Court of City and County of San Francisco*, 387 U. S. 523 (1967) (home administrative search). The doctrine permits intrusions into a person's body and home, areas afforded the greatest Fourth Amendment protection. But there were no such intrusions here.

"[O]ne's expectation of privacy in an automobile and of freedom in its operation are significantly different from the traditional expectation of privacy and freedom in one's residence." *Martinez-Fuerte*, *supra*, at 561. This is because "[a]utomobiles, unlike homes, are subjected to pervasive and continuing governmental regulation and controls." *South Dakota* v. *Opperman*, 428 U. S. 364, 368 (1976); see also *New York* v. *Class*, 475 U. S. 106, 113 (1986) ("[A]utomobiles are justifiably the subject of pervasive regulation by the State"); *Cardwell* v. *Lewis*, 417 U. S. 583, 590 (1974) ("One has a lesser expectation of privacy in a motor vehicle because its function is transportation and it seldom serves as one's residence or as the repository of personal effects"). The lowered expectation of privacy in one's automobile is coupled with the limited nature of the intrusion: a brief, standardized, nonintrusive seizure.[6] The brief seizure of an automobile can hardly be compared to the intrusive search of the body or the home. Thus, just as the "special needs" inquiry serves to both define and limit the permissible scope of those searches, the *Brown* v. *Texas* balancing test serves to define and limit the permissible scope of automobile seizures.

Because of these extrinsic limitations upon roadblock seizures, the Court's newfound non-law-enforcement primary purpose test is both unnecessary to secure Fourth Amendment rights and bound to produce wide-ranging litigation over the "purpose" of any given seizure. Police designing highway roadblocks can never be sure of their validity, since a jury might later determine that a forbidden purpose exists. Roadblock stops identical to the one that we upheld in *Sitz* 10 years ago, or to the one that we

---

[6]This fact distinguishes the roadblock seizure of an automobile from an inventory search of an automobile. Cf. *Colorado* v. *Bertine*, 479 U. S. 367 (1987) (automobile inventory search).

upheld 24 years ago in *Martinez-Fuerte*, may now be challenged on the grounds that they have some concealed forbidden purpose.

Efforts to enforce the law on public highways used by millions of motorists are obviously necessary to our society. The Court's opinion today casts a shadow over what had been assumed, on the basis of *stare decisis*, to be a perfectly lawful activity. Conversely, if the Indianapolis police had assigned a different purpose to their activity here, but in no way changed what was done on the ground to individual motorists, it might well be valid. See *ante*, at 14, n. 2. The Court's non-law-enforcement primary purpose test simply does not serve as a proxy for anything that the Fourth Amendment is, or should be, concerned about in the automobile seizure context.

Petitioners' program complies with our decisions regarding roadblock seizures of automobiles, and the addition of a dog sniff does not add to the length or the intrusion of the stop. Because such stops are consistent with the Fourth Amendment, I would reverse the decision of the Court of Appeals.

SUPREME COURT OF THE UNITED STATES

No. 99–1030

CITY OF INDIANAPOLIS, ET AL., PETITIONERS *v.*
JAMES EDMOND ET AL.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SEVENTH CIRCUIT

[November 28, 2000]

JUSTICE THOMAS, dissenting.

Taken together, our decisions in *Michigan Dept. of State Police* v. *Sitz,* 496 U. S. 444 (1990), and *United States* v. *Martinez-Fuerte,* 428 U. S. 543 (1976), stand for the proposition that suspicionless roadblock seizures are constitutionally permissible if conducted according to a plan that limits the discretion of the officers conducting the stops. I am not convinced that *Sitz* and *Martinez-Fuerte* were correctly decided. Indeed, I rather doubt that the Framers of the Fourth Amendment would have considered "reasonable" a program of indiscriminate stops of individuals not suspected of wrongdoing.

Respondents did not, however, advocate the overruling of *Sitz* and *Martinez-Fuerte,* and I am reluctant to consider such a step without the benefit of briefing and argument. For the reasons given by THE CHIEF JUSTICE, I believe that those cases compel upholding the program at issue here. I, therefore, join his opinion.

Read 10/18 in class

December 15, 2002

Total Information Awareness

By JEFFREY ROSEN

Early this year, the Department of Defense disclosed the most sweeping effort to monitor the activity of Americans since the 1960's, a program called Total Information Awareness. The T.I.A. program is the Bush administration's most visible attempt to implement an idea that became ascendent after 9/11: that the best way to catch terrorists is to allow federal agencies to share information about American citizens and aliens that is currently stored in separate databases. When Congress created the Department of Homeland Security, for instance, it pledged to share data with state and local officials that is currently maintained by the F.B.I. and the C.I.A.

lol

But the Total Information Awareness program takes the principle of information-sharing to a new level. Directed by John Poindexter, the former national security adviser to President Reagan whose conviction for lying to Congress was overturned on appeal, the T.I.A. program seeks to "revolutionize the ability of the United States to detect, classify and identify foreign terrorists" by developing data-mining and profiling technologies that could analyze commercial transactions and private communications.

According to its Web site, which features a Latin slogan that means "knowledge is power," "Total Information Awareness of transnational threats requires keeping track of individuals and understanding how they fit into models." To this end, T.I.A. seeks to develop architectures for integrating existing databases into a "virtual, centralized, grand database." In addition to analyzing financial, educational, travel and medical records, as well as criminal and other governmental records, the T.I.A. program could include the development of technologies to create risk profiles for millions of visitors and American citizens in its quest for suspicious patterns of behavior.

meh

Civil libertarians greeted T.I.A. with alarm and called it a harbinger of even more Orwellian technologies to come. "I fully believe that data-mining in the next five years will be used to determine whether you or I get access to a federal office building," said Marc Rotenberg of the Electronic Privacy Information Center. The Bush administration stands behind T.I.A., but privacy advocates hope to persuade Congress to pull the plug. When the government proposed creating a National Data Center in 1965, public outcry led to the passage of the Privacy Act of 1974, which prohibits federal agencies from routinely sharing personal information. Whether Americans still support that principle after 9/11 remains to be seen.

Oh really - did not know