ABA Standards for Criminal Justice

Third Edition

Law Enforcement Access to Third Party Records

Library of Congress Control Number: 2013943508
ISBN: 978-1-62722-167-2

The commentary contained herein does not necessarily represent the official position of the ABA. Only the text of the black-letter standards has been formally approved by the ABA House of Delegates as official policy. The commentary, although unofficial, serves as a useful explanation of the black-letter standards.

Project of the
American Bar Association
Criminal Justice Standards Committee
Criminal Justice Section
1050 Connecticut Ave., NW, Suite 400
Washington, D.C. 20036
202/662-1500
http://www.americanbar.org/groups/criminal_justice.html

Jane Messmer, Section Director
Kevin Scruggs, Project Director

Printed in the United States of America

ABA Standards for Criminal Justice

Third Edition

Law Enforcement Access to Third Party Records

Leadership During Project

ABA Criminal Justice Section Chairs

William Shepherd, 2012-2013
Janet Levine, 2011-2012
Bruce Green, 2010-2011
Charles J. Hynes, 2009-10
Anthony Joseph, 2008-09
Stephen A. Saltzburg, 2007-08
Robert M. Johnson, 2006-07

Criminal Justice Standards Committee Chairs

Mark Dwyer, 2011-2013
Martin Marcus, 2008-2011
Irwin Schwartz, 2005-2008

Task Force on Law Enforcement Access to Third Party Records

Michael L. Bender, Chair
Stephen E. Henderson, Reporter

"Black letter" Standards approved by ABA House of Delegates, February 2012

Commentary approved by the Standards Committee, March 2013

ABA Criminal Justice Standards Committee 2012-2013

Chair

Mark Dwyer
New York Supreme Court
Brooklyn, New York

Members

Erin H. Becker
King County Prosecuting Attorney's Office
Seattle, Washington

John D. Cline
Law Offices of John D. Cline
San Francisco, California

James W. Cooper
Arnold & Porter LLP
Washington, D.C.

Sam Kamin
Sturm College of Law
Denver, Colorado

Martin Marcus
New York Supreme Court
Bronx, New York

Matthew F. Redle
Sheridan County Prosecuting Attorney
Sheridan, Wyoming

Pauline Weaver
Law Office of Pauline Weaver
Fremont, California

Kym L. Worthy
Wayne County Prosecutor
Detroit, Michigan

Liaisons

John Wesley Hall
National Association of Criminal Defense Lawyers
Little Rock, Arkansas

Jason Lamb
National District Attorneys Association
Jefferson City, Missouri

Daniel J. Lenerz
U.S. Department of Justice
Washington, D.C.

Margaret Colgate Love
National Legal Aid and Defender Association
Washington, D.C.

Standards Committee Staff

Kevin Scruggs
Shamika Dicks
Washington, D.C.

During the Standards Committee consideration of this edition of the Standards, the Committee was also chaired by Marty Marcus (2008-2011) of Bronx, New York. Also serving as Committee members during the review period were: Anthony Joseph, Birmingham, Alabama; Cheryl Jacobs, Baltimore, Maryland; Nancy King, Nashville, Tennessee; Harlan Levy, New York, New York; Theodore McKee, Philadelphia, Pennsylvania; Peter Pope, New York, New York.

Law Enforcement Access to Third Party Records

Chair

Michael L. Bender
Chief Justice, Colorado Supreme Court
Denver, Colorado

Reporter

Stephen E. Henderson
The University of Oklahoma College of Law
Norman, Oklahoma

Members

Norman Frink
Office of the Multnomah County District Attorney
Portland, Oregon

Samuel Guiberson
Guiberson Law Office
Houston, Texas

Albert J. Krieger
Albert J. Krieger, P.A.
Miami, Florida

Gary Lacey
Lancaster County Attorney
Lincoln, Nebraska

Paul Ohm
University of Colorado Law School
Boulder, Colorado

Christopher Slobogin
Vanderbilt University Law School
Nashville, Tennessee

Andrew Taslitz
American University, Washington College of Law
Washington, D.C.

Liaisons

Richard W. Downing
U.S. Department of Justice
Washington, D.C.

David Larson
Federal Bureau of Investigation
Washington, D.C.

Timothy P. O'Toole
Miller & Chevalier
Washington, D.C.

Martin Pinales
National Association of Criminal Defense Lawyers
Cincinnati, Ohio

Task Force Staff

Susan W. Hillenbrand
Washington, D.C.

Future Revisions, Additions or Deletions Related to These Standards

The "black letter" Standards in this publication constitute ABA policy until and unless superseded. Any revisions, additions or deletions related to these Standards will be noted on the ABA Criminal Justice Section website. Please check the website to confirm the most recent version.

Current ABA Criminal Justice Standards

Collateral Sanctions and Discretionary Disqualification of Convicted Persons, ©2004
Criminal Appeals, ©1980; 1986 supp. (out of print)
Discovery and Trial by Jury, ©1996
DNA Evidence, ©2007
Electronic Surveillance: *Section A: Private Communications*, ©2002
Electronic Surveillance: Section B: Technologically-Assisted Physical Surveillance, ©1999
Fair Trial and Free Press, ©1992 (being updated)
Joinder & Severance, ©1980, 1986 supp. (out of print)
Mental Health, ©1986, 1989 (being updated)
Pleas of Guilty, ©1999
Postconviction Remedies, ©1980, 1986 supp. (out of print; being updated)
Pretrial Release, ©2007
Prosecution Function and Defense Function, ©1993 (being updated)
Providing Defense Services, ©1992
Sentencing, ©1994
Special Functions of the Trial Judge, ©2000
Speedy Trial and Timely Resolution of Criminal Cases, ©2006
Treatment of Prisoners, ©2011

Current Standards Drafting Projects

Diversion and Specialized Courts (new)
Fair Trial and Free Press (update)
Mental Health (update)
Monitors (new)
Prosecution and Defense Function (update)
Prosecutorial Investigations (update)
Post-Conviction Remedies (update)

Order information, on-line access to the current Standards, and other information about the Standards project can be found at: http://www.americanbar.org/groups/criminal_justice/policy/standards.html.

ABA Standards for Criminal Justice
Law Enforcement Access to Third Party Records

Table of Contents

Part V. Access to Records

Part VI. Retention, Maintenance, and Disclosure of Records

Part VII. Accountability

INTRODUCTION

Background of the Standards

Approximately forty years ago, the American Bar Association ("ABA") published the initial volumes of its Criminal Justice Standards.[1] One of those initial Standards was that relating to Electronic Surveillance, providing detailed guidelines for the interception of the contents of private communications.[2] Now in its Third Edition,[3] those Standards guide access to telephone, e-mail, and oral communications legally governed by the federal Wiretap Act,[4] the federal Stored Communications Act,[5] and related state laws. More recently, in 1999, the ABA promulgated a "Section B" relating to Technologically-Assisted Physical Surveillance.[6] Those Standards guide law enforcement physical surveillance that is technologically enhanced, divided into the four categories of video surveillance, tracking devices, illumination and telescopic devices, and detection devices.

For some time, the ABA has planned to address another form of law enforcement information gathering: obtaining existing records from third party entities such as banks, hospitals, and internet service providers.[7] Thus, in late 2006, the ABA's Criminal Justice Standards Committee appointed a Task Force to develop these guidelines. On March 16, 2010, after three years of work, the Task Force forwarded its proposed Standards to the Criminal Justice Standards Committee. After revision,

1. *See* Martin Marcus, *The Making of the ABA Criminal Justice Standards: Forty Years of Excellence*, 23 Crim. Just. 10, 10 (2009).

2. ABA Standards for Criminal Justice, Electronic Surveillance (1st ed. 1971).

3. ABA Standards for Criminal Justice, Electronic Surveillance, Section A: Electronic Surveillance of Private Communications (3d ed. 2001).

4. 18 U.S.C. §§ 2510-2522.

5. 18 U.S.C. §§ 2701-2712.

6. ABA Standards for Criminal Justice, Electronic Surveillance, Section B: Technologically-Assisted Physical Surveillance (1999).

7. *See* ABA Standards for Criminal Justice, Electronic Surveillance, Section A, *supra* note 3, at 6-7; ABA Standards for Criminal Justice, Electronic Surveillance, Section B, *supra* note 6, at 2.

on June 20, 2011, the Standards Committee approved the proposed Standards and forwarded them to the Criminal Justice Section Council and other interested parties. After further revision, the Section Council approved the proposed Standards at their second reading on October 29, 2011. At the ABA midyear meeting on February 6, 2012, the House of Delegates adopted these Standards as the twenty-fifth volume of the ABA Standards for Criminal Justice.

Need for the Standards

Government access to third party records is not novel. Indeed, law enforcement seeking evidence of crime in records maintained by non-governmental institutions is surely among the most important and common investigatory activities. The federal government and all fifty states regulate government access to and use of certain types of record information.[8] Every criminal procedure student learns the series of relevant Fourth Amendment cases from the 1960s to 1980s.[9] But because the federal constitutional regulation has historically been slight, and because other regulation has occurred in an *ad hoc* manner, there is no existing framework via which legislatures, courts acting in their supervisory capacities, and agencies can make the difficult decisions regarding what records should be protected and the scope of such protection.

Moreover, with the maturation of digital storage and search technologies, and virtually costless distributions, we now live in a world of ubiquitous third party information.[10] Although data can of course

8. *See, e.g.*, 9 C.J.S. Banks and Banking § 269 (summarizing restrictions on government access to bank records); Tracy A. Bateman, *Search and Seizure of Bank Records Pertaining to Customer as Violation of Customer's Rights Under State Law*, 3 A.L.R.5th 453 (1995).

9. *See* A Comment on the Fourth Amendment, *infra*.

10. In the words of Judge Richard Posner,

> [A] person would have to be a hermit to be able to function in our society without voluntarily disclosing a vast amount of personal information to a vast array of public and private demanders. This has long been true, but until quite recently the information that people voluntarily disclosed to vendors, licensing bureaus, hospitals, public libraries, and so forth, was scattered, fugitive (because the bulkiness of paper records usually causes them to be discarded as soon as they lose their value to the enterprise), and searchable only with great difficulty. So although one had voluntarily disclosed private information on innumerable occasions to sundry recipients, one retained as a practical matter a great deal of privacy. But with digitization, not only can recorded information be retained indefinitely at little cost,

be scrubbed and is routinely overwritten, it is nonetheless difficult to overstate the magnitude of information that now resides with third parties, from our shopping preferences (residing with our credit and debit card providers and individual stores), to our communications (residing with our service providers and other intermediaries), to our health information (residing with doctors, pharmacies, hospitals, and insurance companies), to our viewing habits (residing with our cable and internet providers), to our very location (residing with our mobile phone providers and toll tag operators).

Whole categories of data are stored that never were before. Not long ago, if a customer made a purchase with cash, a bookstore often would have made no individualized record of what was bought. Similarly, a library would have recorded only the materials ultimately checked out. But when we browse online, including bookstores and libraries, multiple service providers might record every article, picture, book and video that we peruse. Whereas in a store purchase in an earlier day a clerk might recognize or remember a face and some of the items purchased, today when we purchase with "discount" or "customer loyalty" cards, the store records everything purchased, no matter the location or time of sale. If we purchase online, the store might record everything we even consider purchasing and store this information for as long as it is considered financially or legally beneficial. Whereas one used to anonymously pick up the broadcast television signal with an antenna, today our provider often knows what we watch and when. Whereas we used to store computer files on our home computers, many now store them instead on third party servers, taking advantage of so-called "cloud computing."

These trends have critical implications for both law enforcement and privacy. Access to such records deters and detects crimes as diverse as kidnapping (phone records), public corruption and organized crime (bank records), and child sexual assault (internet records). Even a seemingly "routine" street crime might depend upon records access for resolution, as when hospital admission records allow police to discover

---

but also the information held by different merchants, insurers, and government agencies can readily be pooled, opening the way to assembling all the recorded information concerning an individual in a single digital file that can easily be retrieved and searched.

Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. Chi. L. Rev. 245, 248 (2008).

who might have been involved in a recent shooting, or when toll tag records allow police to learn the culprit in a fatal hit-and-run. Moreover, records access permits law enforcement to deter or punish private access that is itself harmful and criminal, such as identity theft and computer hacking. To paraphrase Judge Richard Posner, secrecy is the criminal's best friend.[11]

When evidence is available via third party records, records access has the additional benefit of not risking a physical confrontation with the target. When police enter a home or otherwise seek to forcibly obtain information directly from a suspect, there is always a threat of violence and therefore of harm either to the police, to bystanders, or to the suspect him- or herself. The ability to obtain evidence from a neutral third party eliminates this risk. Similarly, while a prosecutor might subpoena records from a suspect, that risks their destruction despite the threat of criminal liability for obstruction. Once again, third party records access largely eliminates that risk.

Of course, such law enforcement access implicates privacy. At information privacy's core is an ability to control what information about you is conveyed to others, and for what purposes.[12] American norms of limited

11. *See id*. at 251 ("Privacy is the terrorist's best friend.").

12. Alan Westin's seminal 1967 work stated this principle as follows: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Alan F. Westin, Privacy and Freedom 7 (Antheneum 1967). *See* Shaktman v. State, 553 So.2d 148, 150 (Fla. 1989) (adopting this definition). More recently Westin writes that "[m]ost definitions of privacy agree on a core concept: that privacy is the claim of an individual to determine what information about himself or herself should be known to others. This also involves when such information will be communicated or obtained and what uses will be made of it by others." Alan F. Westin, *Historical Perspectives on Privacy: From the Hebrews and Greeks to the American Republic* 4 (presented and distributed at the 2009 Privacy Law Scholars Conference, and quoted with permission).

To Charles Fried, "[P]rivacy [i]s that aspect of social order by which persons control access to information about themselves." Charles Fried, *Privacy*, 77 Yale L. J. 475, 493 (1968). One of the key themes in Samuel Warren and Louis Brandeis's seminal 1890 article was each individual's "right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others." Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 198 (1890). Andrew Taslitz has similarly explained that: "[e]ach of us wears many masks wherein each mask reflects a different aspect of who we really are. . . . [W]e want to choose the masks that we show to others; any such loss of choice is painful, amounting almost to a physical violation of the self. When we are secretly watched, or when information that we choose to reveal

government and principles of freedom of speech and association thus require that law enforcement records access be regulated. Courts, legislatures, and administrative agencies are struggling to determine when law enforcement access to medical records, location, and other information should be permissible, and these Standards provide a framework via which they can bring greater consistency to existing law, and, where necessary, frame new law that accounts for changing technologies and social norms, the needs of law enforcement, and the interests of privacy, freedom of expression, and social participation.

Scope of the Standards

These Standards relate to law enforcement investigatory access to, and storage and disclosure of, records maintained by institutional third parties. In other words, they address government agents seeking to acquire evidence from existing records to be used in the detection, investigation, or prevention of crime.

The Standards do not address access for purposes of national security. Although access to records can be critical to keeping our country safe from foreign attack, and such access can also be abused, these Standards follow the lead of previous Standards in not addressing records acquisition intended to acquire information concerning a foreign power or an agent thereof.[13] This would include not only information directly relating to such a foreign agent, but information relevant to a legitimate investigation of such agent.[14] If information is lawfully gathered for a

---

to one audience is instead exposed to another, we lose that sense of choice." Andrew E. Taslitz, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions*, 65 Law & Contemp. Probs. 125, 131 (2002).

13. *See, e.g.*, ABA Standards for Criminal Justice, Electronic Surveillance, Section A: Electronic Surveillance of Private Communications, 5-6 (3d ed. 2001).

14. Prior to passage of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (the "Patriot Act"), the statutory national security carve-out was limited to information pertaining to a foreign power or an agent of a foreign power. *See e.g.*, 18 U.S.C. § 2709(b)(1)(B) (effective October 21, 1986 to October 25, 2001) (permitting access to certain telephone records). Today, according to section 505 of the Patriot Act, the carve-out is more generous, in that the information must be "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States." 18 U.S.C. § 2709(b)(1). In other words, the national security carve-out now

national security purpose, these Standards do not imply anything concerning its use in a criminal investigation. Again, they simply do not address access for purposes of national security.

The Standards also do not address records access for purposes of civil investigations, nor for criminal prosecutions. These standards regulate investigatory law enforcement access, not access following the initiation and in the course of a criminal prosecution. Once adversary judicial proceedings have commenced, there are constitutional guarantees to counsel and judicial oversight that do not exist prior to formal charge.

In order to give deference to the historically favored status of grand juries, the Standards also do not address records access via a grand jury subpoena. In many jurisdictions where investigative grand juries are not typically used, there is a comparable history of using functionally equivalent prosecutorial subpoenas in their place. These too are therefore carved out of the Standards.

The Standards also do not address records access from an individual not acting as a business entity. Not only does such an individual have an autonomy interest in choosing to share information with law enforcement, but the motivating concern of these Standards is the much more significant threat to privacy in the ever-increasing amounts of information contained within systems of records maintained by entities.

Finally, the Standards do not address acquisition of information contemporaneous with its generation or transmission (e.g., a wiretap), as such real-time access is already the province of other Standards.

A Comment on the Fourth Amendment

Although the Fourth Amendment "third party doctrine" is complicated and contested,[15] in a series of cases beginning in the 1960s and continuing into the 1980s, the Supreme Court developed the doctrine that one typically retains no federal constitutional reasonable expectation of privacy in information conveyed to a third party.[16] Of course, the

includes telephone records of a person who is *not* an agent of a foreign power, so long as those records are relevant to a national security investigation of such an agent.

15. *Cf.* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561 (2009); Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 Iowa L. Rev. Bull. 39 (2011).

16. These are the "false friend" cases of *Hoffa v. United States*, 385 U.S. 293 (1966), and *United States v. White*, 401 U.S. 745 (1971); the bank records case of *United State v. Miller*,

doctrine is not absolute, as the Court granted constitutional protection to the contents of telephone conversations conveyed to a third party provider,[17] and lower federal courts have therefore granted constitutional protection to reading preferences,[18] medical information,[19] and electronic mail.[20] Thus, the Supreme Court has urged caution:

> Th[is] Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment . . . . The judiciary risks

425 U.S. 435 (1976); the phone records case of *Smith v. Maryland*, 442 U.S. 735 (1979); the beeper cases of *United States v. Knotts*, 460 U.S. 276 (1983), and *United States v. Karo*, 468 U.S. 705 (1984); the flyover cases of *California v. Ciraolo*, 476 U.S. 207 (1986), and *Florida v. Riley*, 488 U.S. 455 (1989); the open fields cases of *Oliver v. United States*, 466 U.S. 170 (1984), and *United States v. Dunn*, 480 U.S. 294 (1987); and the garbage case of *California v. Greenwood*, 486 U.S. 35 (1988). In the words of the *Miller* Court,

> [We] ha[ve] held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by [the third party] 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.

425 U.S. at 443. A third party of course potentially retains its *own* reasonable expectation of privacy in the information, and can assert those Fourth Amendment interests.

17. *See* Berger v. New York, 388 U.S. 41 (1967); Katz v. United States, 389 U.S. 347 (1967). The particular situation in *Katz* can be distinguished in that the information at issue was not obtained via the third party, but typically the Constitution treats information identically whether it is acquired directly by the government or historically via the third party (e.g., pen register and trap and trace). The point is merely that the Court has never addressed why telephone content information would not fall within the third party doctrine were it provided by the third party. *See* Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 Mercer L. Rev. 507, 524-29 (2005) (thus articulating a "limited third party doctrine").

18. *See* Amazon.com v. Lay, 758 F. Supp.2d 1154, 1167- 69 (W.D. Wash. 2010) (rejecting government subpoena of records documenting book, music, and movie purchases); In re Grand Jury Investigation of Possible Violation of 18 U.S.C. Section 1461, 706 F. Supp. 2d 11, 16-23 (D.D.C. 2009) (rejecting grand jury subpoena of records documenting movie purchases); In re Grand Jury Subpoena to Amazon.com Dated August 7, 2006, 246 F.R.D. 570, 572-74 (W.D. Wis. 2007) (rejecting grand jury subpoena of records documenting book purchases).

19. *See* Doe v. Broderick, 225 F.3d 440 (4th Cir. 2000) (requiring a warrant to access medical/prescription records); State v. Skinner, 10 So. 3d 1212 (La. 2009) (same); Commonwealth v. Riedel, 539 Pa. 172 (1994) (finding a reasonable expectation of privacy in medical records and requiring probable cause but no warrant). *Cf.* People v. Perlos, 436 Mich. 305 (1990) (finding no reasonable expectation of privacy).

20. *See* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

> error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. . . . Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. . . . At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve. . . . Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy.[21]

Most recently, when the Court unanimously held that the Fourth Amendment restricts law enforcement long-term GPS tracking of automobiles, Justice Sotomayor more generally questioned the wisdom of the third party doctrine given modern technologies:

> 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. 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. . . . 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 to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the

21. City of Ontario v. Quon, 130 S. Ct. 2619, 2629-30 (2010).

> public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[22]

Fortunately, it is not necessary for purposes of these Standards to answer these constitutional questions. Although decision makers will of course be bound by constitutional decisions (see Standard 25-2.2), the Standards do not purport to interpret the federal constitution nor any state equivalent,[23] nor the many statutes and administrative regulations that regulate law enforcement access to third party records.[24] They instead carefully consider all of these, and other sources, in providing a framework via which decision makers, including legislatures, courts acting in their supervisory capacities, and administrative agencies, can answer such questions, thereby thoughtfully and consistently regulating government access to third party records.

Organization of the Standards

Part I provides definitions used throughout the Standards. The contents of Parts II and III were described above: Part II delimits the Standards' scope, and Part III articulates the general governing principles. Parts IV, V, and VI then provide the substantive recommendations, Part IV governing the categorization and protection of information, Part V the access to records, and Part VI record retention, maintenance, and disclosure following that access. Part VII then provides accountability for those substantive recommendations.

In many ways, Part IV is the heart of the Standards. A decision maker, often a legislature but also potentially a court acting in its supervisory

22. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (internal citations omitted).

23. Some states have constitutional protection exceeding that of the federal Fourth Amendment. For a summary of that law see Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 Pepp. L. Rev. 975 (2007); Stephen E. Henderson, *Learning from All Fifty States: How To Apply the Fourth Amendment and Its State Analogs To Protect Third Party Information from Unreasonable Search*, 55 Cath. U. L. Rev. 373 (2006).

24. For example, when the Supreme Court has refused Fourth Amendment protection, Congress has sometimes enacted statutory regulation. Thus, when the Supreme Court found no Fourth Amendment protection for bank records, Congress responded via the Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422. When the Court found no constitutional protection for telephone numbers dialed, Congress likewise granted statutory protection. *See* 18 U.S.C. §§ 3121-3127.

capacity or an administrative agency,[25] first determines the level of privacy for a given category of information.[26] For example, should records of banking transactions be considered *highly private*, *moderately private*, *minimally private*, or *not private*? The Standards provide four important criteria that should be considered in making this determination, in addition to considering the relevance of present and developing technology.[27] The Standards do not, however, suggest a particular answer, thus respecting local circumstances, changing needs, and the necessarily difficult nature of this inquiry.

Once this degree of privacy is determined, it sets a threshold level of protection: highly private records are highly protected, moderately private records are moderately protected, etc.[28] Absent consent, emergency aid, or exigent circumstances; consistent with the law of privilege;[29] and absent any greater constitutional protection; law enforcement should be permitted to access a highly protected record via a warrant supported by probable cause.[30] For moderately protected information, access should require a court order supported by reasonable suspicion or, if the legislature or other decision maker so chooses, a court order supported by relevance or issued pursuant to a prosecutorial certification.[31] Access to minimally protected information should require a prosecutorial or agency determination of relevance.[32] And access to unprotected information should be permissible for any legitimate law enforcement purpose.[33]

Although the privacy of a category of records alone sets this threshold, there may be circumstances in which that threshold makes it too difficult to solve crime. In that case, the legislature or other decision maker should reduce the level of protection accordingly.[34] The Standards also

25. A legislature can use the standards in formulating legislation, a police department can use them in formulating administrative rules, and, where doing so is consistent with its supervisory role, a court can use them in determining "common law."
26. *See* Standard 25-4.1.
27. *See id.*
28. *See* Standard 25-4.2(a).
29. *See* Standard 25-5.3(c).
30. *See* Standard 25-5.3(a)(i).
31. *See* Standard 25-5.3(b)(ii).
32. *See* Standard 25-5.3(b)(iii).
33. *See* Standard 25-5.3(d).
34. *See* Standard 25-4.2(b).

provide for access to inclusive bodies of de-identified records (that is, records not linkable through reasonable efforts to an identifiable person) upon which law enforcement has reason to conduct data mining.[35] Finally, if the record is highly or moderately protected, but not if it has a lesser level of protection, law enforcement should typically ultimately provide notice to the focus of the record, but that notice can be, and often will be, delayed.[36]

Examples

For a hypothetical, consider a local park on a summer evening. Later estimates are that approximately thirty persons were present. At 6:45 pm, the 911 dispatcher receives a cellular call from an unidentified male reporting that "a girl is shot and hurt real bad at Shadyside," the name of the park, after which the caller hangs up. Police begin to arrive by 7:00, but most of the crowd has dispersed. A young woman in jogging clothes is found dead from what is later determined to be a single gunshot wound to the head. Forensics recover numerous rounds of ammunition from the surrounding area, representing several different caliber firearms. Those who remain are questioned by police, but all claim not to have seen anything more detailed than "a bunch of people shooting and screaming."

One person of interest is the 911 caller: even if a mere bystander, he was close enough to know that the victim was female, and might therefore have further information of interest. It would be helpful to know not only his identity, in order to locate him, but also from where the call originated and with whom he communicated near the time of the shooting.

The 911 call center will have automatically recorded an incoming phone number. With that number, the service provider—whether it be AT&T, Sprint, Verizon, or another—will typically be able to provide the desired information.[37] What should be required of law enforcement in order to obtain that information? According to Standard 25-4.1, the first

35. *See* Standard 25-5.6.

36. *See* Standard 25-5.7.

37. If the phone were an entirely prepaid one purchased with cash, obviously this might be a dead end. Because the purpose of this section is merely to demonstrate use of the standards rather than to exhaustively consider investigation of a particular crime, such nuances and many potential investigative leads will go unmentioned.

question is how private is the desired information. In other words, is a subscriber's identity *highly private*, *moderately private*, *minimally private*, or *not private*? What about the telephone numbers of those whom he called? And what about his geographic location, determined if nothing else by his proximity to a particular cell tower at the time of the call?

These can be difficult questions, but the Standards provide four factors a decision maker should use in this determination. It should be stressed that this determination will have been made by a legislature, administrative agency, or court. It is *not* an officer on the beat who would be considering these factors. The factors are the extent to which:

(a) the initial transfer of such information to an institutional third party is reasonably necessary to participate meaningfully in society or in commerce, or is socially beneficial, including to freedom of speech and association;

(b) such information is personal, including the extent to which it is intimate and likely to cause embarrassment or stigma if disclosed, and whether outside of the initial transfer to an institutional third party it is typically disclosed only within one's close social network, if at all;

(c) such information is accessible to and accessed by non-government persons outside the institutional third party; and

(d) existing law, including the law of privilege, restricts or allows access to and dissemination of the information or of comparable information.[38]

Without going into great detail—and keep in mind the Standards do not purport to *answer* this question for legislatures or other deliberative bodies—this limited information, including location at one particular time, might be minimally private. Consider the telephone numbers of those called. On the one hand, telephone conversations have long furthered the freedoms of expression and association, and they seem necessary to participate meaningfully in society.[39] And while they are not as

38. Standard 25-4.1.

39. In *Katz v. United States*, 389 U.S. 347, 352 (1967), the Court recognized "the vital role that the . . . telephone has come to play in private communication," and several courts have more recently recognized the same in the context of determining state constitutional protections. *See* People v. Chapman, 679 P.2d 62, 67 (Cal. 1984) ("Doing without a telephone is not a realistic option for most people."); People v. Sporleder, 666 P.2d 135, 141 (Colo. 1983) ("A telephone is a necessary component of modern life. It is a personal and business necessity indispensable to one's ability to effectively communicate in today's complex society."); State v. Hunt, 450 A.2d 952, 955-56 (N.J. 1982) ("The telephone has become an essential instrument in carrying on our personal affairs.").

personal as the communications themselves, call records alone form a sort of "virtual biography" in that we are in some sense defined by the entirety of the persons to whom we communicate.[40] And federal law not only restricts law enforcement access to call records,[41] but also public provider voluntary dissemination of those records,[42] and criminalizes fraudulent access by a private person.[43]

So, call records would not be considered "not private." But neither do they seem highly private, as would be the communications contents themselves. So, call records would seem either to be moderately or minimally private, and given the substantive measure of existing protections, and the records' intimacy, perhaps a legislature or other decision maker would consider them minimally private. The threshold would then be that call records are minimally protected, meaning they could be accessed if a prosecutor considers them relevant to the investigation, which he or she certainly would on these facts.

If the police are thereafter interested in a particular conversation that occurred immediately after the 911 call—perhaps because it would disclose further details of the incident and of the caller's involvement therein—and if that conversation was recorded by the service provider (e.g., a voicemail), using the same criteria a legislature might deem the content of communications to be highly protected, in which case law enforcement should need either a warrant supported by probable cause or a grand jury subpoena. Although there is no such indication on these facts, if there were reason to believe that another life was in imminent peril, that content should be accessible via the request of a law enforcement officer or prosecutor.[44] Of course, if a relevant constitutional provision has been interpreted to require a certain restraint, a legislature should not purport to permit access upon a lesser restraint.[45]

Once police have the name of the caller, if they believe he is potentially involved they might want to learn more about him via any internet post-

40. *See* People v. DeLaire, 610 N.E.2d 1277, 1282 (Ill. App. Ct. 1993) ("[T]he [dialing] records revealed personal associations and dealings which create a 'biography' which should not be subject to an unreasonable search or seizure.").

41. *See* 18 U.S.C. § 2703(c)(1).

42. *See* 18 U.S.C. §§ 2702(a)(3), 2702(c); 47 U.S.C. § 222.

43. *See* 18 U.S.C. § 1039.

44. *See* Standard 25-5.4.

45. *See* Standard 25-2.2.

ings, such as those on Facebook,[46] Twitter,[47] and Myspace.[48] So long as the desired content is publicly available on those sites, application of the four factors would almost surely render it *not private* and therefore *unprotected*. It could therefore be accessed by an officer for any legitimate law enforcement purpose.[49]

Police would also want to obtain relevant hospital admission records near the time of the shooting in case anyone else was wounded by the gunfire. Even if medical diagnosis and treatment records might generally be highly protected, such protection for hospital admissions records relating to gunshot wounds is likely to unacceptably interfere with the investigation of crime. In that case, a legislature or other decision maker should reduce the level of protection, including potentially making such information subject to a mandatory reporting law.[50]

What about providing notice to those whose records are obtained? So long as the information is minimally protected, the standards recommend that no notice be required.[51] Were notice required, Standard 25-5.7(b) would permit 30 days within which to provide that notice, and Standard 25-5.7(c) would permit delaying that notice upon reasonable belief that it would jeopardize an investigation, including causing flight from prosecution or tampering with evidence.

Looking ahead, what if another police department in a neighboring jurisdiction experiences a similar shooting, and wants to obtain the records gathered in the first investigation? Regardless of how private are the records, Standard 25-6.2(b) permits access upon official certification, or upon the request of an officer or prosecutor in an emergency or during exigent circumstances. An official certification requires that a politically accountable official put in writing that the record is considered relevant to initiating or pursuing an investigation.[52]

The operation of the Standards is the same for more modern information crimes. If a bank account holder reports to police that her account has been emptied, law enforcement will want to examine her account

46. http://www.facebook.com/ (last accessed June 1, 2011).
47. http://twitter.com/ (last accessed June 1, 2011).
48. http://www.myspace.com/ (last accessed June 1, 2011).
49. *See* Standard 25-5.3(d).
50. *See* Standards 25-4.2(b).
51. *See* Standard 25-5.7(a).
52. *See* Standard 25-5.2(c). "Politically accountable official" is defined in Standard 25-1.1(f).

records. Although information provided by the victim would be sufficient to obtain whatever specific authorization is required by Standard 25-5.3 to access financial account and transaction records, the victim's consent alone would be adequate according to Standard 25-5.1. It might prove necessary to examine computer logs of the bank, especially if the theft appears to be the work of a hacker. Here the customer could not effectively consent because the records do not belong to him or her, but as a victim the bank itself could consent according to Standard 25-2.1(f)(i).

Assuming a hacker has indeed transferred the funds, he or she will typically move them through several accounts in a series. If those accounts are located in a foreign country, then the necessarily more complicated international law will apply. But assuming they are all located in the United States, either those banks could give effective consent as victims under Standard 25-2.1(f)(i), or law enforcement could obtain the necessary authorizations under Standard 25-5.3. For example, if according to the four factors of Standard 25-4.1 the relevant legislature determined financial account and transactional records to be moderately private, pursuant to Standard 25-4.2 they would be moderately protected (assuming such a protection would not unduly cripple law enforcement). According to Standard 25-5.3(a)(ii), law enforcement access would then require a court order supported by either reasonable suspicion, relevance, or a prosecutorial certification of relevance, depending upon which a decision maker chooses to require. Here law enforcement could satisfy the higher threshold of probable cause.

Assuming the victim's bank logged an Internet Protocol address for the hacker, or the victim's personal computer logged such an address if it were hacked, and assuming basic subscriber information is found to be minimally protected, either a prosecutorial or administrative subpoena could be used to obtain that information from the relevant internet service provider.[53] Of course, a hacker would typically have provided false information, but the same authorization would likely also permit learning with whom that person had communicated online,[54] poten-

53. *See* Standards 25-4.2, 25-5.3(a)(iii). This is possible only if the government is technically able to track through the several proxies a hacker would typically use to mask the true origin of his or her communications. Once again, the purpose of this section is merely to demonstrate use of the standards, not to exhaustively consider any particular investigation.

54. *See id.*

tially providing other leads. If the hacker remains active, either on the bank's system or the victim's personal computer, then law enforcement might want to initiate real-time wiretapping, which is beyond the scope of these standards.[55]

Conclusion

The Standards recognize that the consensus concerning law enforcement access to records held by institutional third parties is still developing, but also recognize the critical need for striking the delicate balance between law enforcement's legitimate need for access to such records and the privacy rights of the subjects of those records. By setting forth criteria to be considered in determining whether categories of records should be treated as highly private, moderately private, minimally private, or not private, and in establishing the appropriate level of protection for each category of records, the Standards provide the framework for legislatures and other deliberative bodies to carry out this critical task.

55. *See* Standard 25-2.1(e).

BLACK LETTER

Part I. Definitions

Standard 25-1.1 Definitions

For purposes of these standards:

(a) "Emergency aid" is government conduct intended to eliminate or mitigate what is reasonably believed to be imminent danger of death or serious physical injury.

(b) "Exigent circumstances" are circumstances in which there is probable cause to fear imminent destruction of evidence or imminent flight.

(c) The "focus of a record" is the person or persons to whom the information in a record principally relates.

(d) "Law enforcement" means any government officer, agent, or attorney seeking to acquire evidence to be used in the detection, investigation, or prevention of crime.

(e) An "institutional third party" is:

- **(i) any nongovernmental entity, including one that receives government funding or that acquires information from government sources; and**
- **(ii) any government institution functioning in a comparable capacity, such as a public hospital or a public university.**

(f) A "politically accountable official" is an upper-level law enforcement official or, in the case of a civil investigation, a civil equivalent, who is either elected or appointed by an elected official, or who is specifically designated for this purpose by an elected or appointed official.

(g) A "record" contains information, whether maintained in paper, electronic, or other form, that is linked, or is linkable through reasonable efforts, to an identifiable person. A "de-identified record" contains information that is not so linkable.

Part II. Scope

Standard 25-2.1 Scope

These standards relate to law enforcement investigatory access to, and storage and disclosure of, records maintained by institutional third parties. These standards do not relate to:

(a) access to records for purposes of national security;

(b) access to records after the initiation and in the course of a criminal prosecution;

(c) access to records via a grand jury subpoena, or in jurisdictions where grand juries are typically not used, a functionally equivalent prosecutorial subpoena;

(d) access to records from an individual not acting as an institutional third party;

(e) acquisition of information contemporaneous with its generation or transmission;

(f) an institutional third party:

- **(i) that is a victim of crime disclosing information that is evidence of that crime or that is otherwise intended to protect its rights or property; or**
- **(ii) deciding of its own initiative and volition to provide information to law enforcement.**

Standard 25-2.2 Constitutional floor

A legislature or administrative agency may not authorize a protection less than that required by the federal Constitution, nor less than that required by its respective state Constitution.

Part III. General Principles

Standard 25-3.1 Records available

Institutional third parties maintain records ranging from the most mundane to those chronicling the most personal aspects of people's lives, and when those records are stored digitally, access and distribu-

tion costs are diminished. These records include such things as the content of communications; medical diagnoses, treatments, and conditions; internet browsings; financial transactions; physical locations; bookstore and library purchases, loans, and browsings; other store purchases and browsings; and media viewing preferences.

Standard 25-3.2 Need for records access

Obtaining records maintained by institutional third parties can facilitate, and indeed be essential to, the detection, investigation, prevention and deterrence of crime; the safety of citizens and law enforcement officers; and the apprehension and prosecution of criminals; and can be the least confrontational means of obtaining needed evidence.

Standard 25-3.3 Implications of records access

Law enforcement acquisition of records maintained by institutional third parties can infringe the privacy of those whose information is contained in the records; chill freedoms of speech, association, and commerce; and deter individuals from seeking medical, emotional, physical or other assistance for themselves or others.

Standard 25-3.4 Need for regulation

Legislatures, courts that may act in a supervisory capacity, and administrative agencies should therefore carefully consider regulations on law enforcement access to and use of records maintained by institutional third parties. These standards provide a framework for that consideration.

Part IV. Categorization of Information and Protection

Standard 25-4.1 Categories of information

Types of information maintained by institutional third parties should be classified as *highly private*, *moderately private*, *minimally private*, or *not private*. In making that determination, a legislature,

court, or administrative agency should consider present and developing technology and the extent to which:

(a) the initial transfer of such information to an institutional third party is reasonably necessary to participate meaningfully in society or in commerce, or is socially beneficial, including to freedom of speech and association;

(b) such information is personal, including the extent to which it is intimate and likely to cause embarrassment or stigma if disclosed, and whether outside of the initial transfer to an institutional third party it is typically disclosed only within one's close social network, if at all;

(c) such information is accessible to and accessed by non-government persons outside the institutional third party; and

(d) existing law, including the law of privilege, restricts or allows access to and dissemination of such information or of comparable information.

Standard 25-4.2 Categories of protection

(a) The type of authorization required for obtaining a record should depend upon the privacy of the type of information in that record, such that: records containing *highly private* information should be *highly protected*, records containing *moderately private* information should be *moderately protected*, records containing minimally private information should be *minimally protected*, and records containing information *that is not private* should be *unprotected*. If a record contains different types of information, it should be afforded the level of protection appropriate for the most private type it contains.

(b) If the limitation imposed by subdivision (a) would render law enforcement unable to solve or prevent an unacceptable amount of otherwise solvable or preventable crime, such that the benefits of respecting privacy are outweighed by this social cost, a legislature may consider reducing, to the limited extent necessary to correct this imbalance, the level of protection for that type of information, so long as doing so does not violate the federal or applicable state constitution.

Part V. Access to Records

Standard 25-5.1 Consent

Law enforcement should be permitted to access by particularized request any record maintained by an institutional third party if:

(a) the focus of the record has knowingly and voluntarily consented to that specific law enforcement access;

(b) the focus of the record has knowingly and voluntarily given generalized consent to law enforcement access, and

(i) the information in the record is unprotected or minimally protected;

(ii) it was possible to decline the generalized consent and still obtain the desired service from the provider requesting consent, and the focus of the record had specifically acknowledged that it was possible; or

(iii) a legislature has decided that in a particular context, such as certain government contracting, generalized consent should suffice for the information contained in the record; or

(c) the record pertains to a joint account and any one joint account holder has given consent as provided in subdivision (a) or (b).

Standard 25-5.2 Types of authorization

When authorization for accessing a record is required pursuant to Standard 25-5.3, it should consist of one of the following, each of which must particularly describe the record to be obtained:

(a) a *court order,* based upon:

(i) a judicial determination that there is probable cause to believe the information in the record contains or will lead to evidence of crime;

(ii) a judicial determination that there is reasonable suspicion to believe the information in the record contains or will lead to evidence of crime;

(iii) a judicial determination that the record is relevant to an investigation; or

(iv) a prosecutorial certification that the record is relevant to an investigation.

(b) a *subpoena*, based upon a prosecutorial or agency determination that the record is relevant to an investigation; or

(c) an *official certification*, based upon a written determination by a politically accountable official that there is a reasonable possibility that the record is relevant to initiating or pursuing an investigation.

Standard 25-5.3 Requirements for access to records

(a) Absent more demanding constitutional protection, consent pursuant to Standard 25-5.1, and emergency aid and exigent circumstances pursuant to Standard 25-5.4; and consistent with the privilege requirements of Standard 5.3(c); law enforcement should be permitted to access a record maintained by an institutional third party pursuant to the following authorization:

(i) a court order under 5.2(a)(i) if the record contains highly protected information;

(ii) a court order under 5.2(a)(ii) [5.2(a)(iii) or 5.2(a)(iv)] if the record contains moderately protected information; or

(iii) a subpoena under 5.2(b) if the record contains minimally protected information.

(b) If the record contains highly protected information, a legislature, a court acting in its supervisory capacity, or an administrative agency could consider more demanding restraints for access to the record, such as additional administrative approval, additional disclosure, greater investigative need, or procedures for avoiding access to irrelevant information.

(c) The protections afforded to privileged information contained in records maintained by institutional third parties and the responsibilities of privilege holders to assert those privileges are those provided by the law applicable in the jurisdiction in which privilege is asserted. The jurisdiction in which law enforcement obtains documents may impose obligations on both institutional third parties to protect what might be privileged information and on law enforcement with respect to the access to, and storage and disclosure of, such information.

(d) Law enforcement should be permitted to access unprotected information for any legitimate law enforcement purpose.

(e) Law enforcement should be permitted to substitute a more demanding authorization for a required lesser authorization.

Standard 25-5.4 Emergency aid and exigent circumstances

Law enforcement should be permitted to access a protected record for emergency aid or in exigent circumstances pursuant to the request of a law enforcement officer or prosecutor. As soon as reasonably practical, the officer or prosecutor should notify in writing the party or entity whose authorization would otherwise have been required under Standard 25-5.3.

Standard 25-5.5 Redacted access to records

Legislatures, courts that may act in a supervisory capacity, and administrative agencies should consider how best to regulate:

(a) law enforcement access when only some information in a record is subject to disclosure; and

(b) the use and dissemination of information by law enforcement when a third party provides more information, including more protected information, than was requested.

Standard 25-5.6 De-identified records

(a) Notwithstanding any other provision of this Part, law enforcement should be permitted to access an appropriately inclusive body of de-identified records maintained by an institutional third party pursuant to an official certification.

(b) A de-identified record should be linked to an identifiable person only if law enforcement obtains the authorization required under Standard 25-5.3 for the type or types of information involved. The showing for this authorization may be based on a profile or algorithm.

Standard 25-5.7 Notice

(a) If the accessed record is unprotected or minimally protected, law enforcement should not be required to provide notice of the access.

(b) If the accessed record is highly or moderately protected, law enforcement should provide notice of the access to the focus of the record, and this notice should generally occur within thirty days after acquisition.

(c) The court that authorizes access to the record, or in the case of emergency aid or exigent circumstances the court that would otherwise have been required to authorize access to the record, may delay notice for a specified period, or for an extension thereof, upon its determination that:

(i) there is a reasonable belief that notice would endanger life or physical safety; would cause flight from prosecution, destruction of or tampering with evidence, or intimidation of potential witnesses; or would otherwise jeopardize an investigation; or

(ii) the delay is necessary to comply with other law.

(d) When a court authorizes delayed notice pursuant to Standard 5.7(c), the court may also prohibit the third party from giving notice during that specified period. If law enforcement obtains a record for emergency aid or in exigent circumstances, a law enforcement officer or prosecutor may by written demand prohibit the third party from giving notice for 48 hours.

(e) When protected de-identified records are accessed, notice should be provided to the [general public] [legislature] and should generally occur [prior to] [after] acquisition.

(f) Upon request, a court should be permitted to eliminate or limit the required notice in a particular case where it would be unduly burdensome given the number of persons who must otherwise be notified, taking into consideration, however, that the greater number of persons indicates a greater intrusion into privacy.

Part VI. Retention, Maintenance, and Disclosure of Records

Standard 25-6.1 Retention and maintenance

(a) Protected records lawfully obtained from an institutional third party in the course of law enforcement investigation should be:

(i) reasonably secure from unauthorized access; and

(ii) other than as authorized under Standard 25-6.2, accessed only by personnel who are involved in the investigation for which they were obtained and only to the extent necessary to carry out that investigation.

(b) Moderately and highly protected records should in addition be:

(i) subject to audit logs recording all attempted and successful access; and

(ii) destroyed according to an established schedule.

(c) All de-identified records in the possession of law enforcement for which the linkage described in Standard 5.6(b) is not obtained should be destroyed upon conclusion of the investigation and any prosecution and appeals.

(d) If a law enforcement agency disseminates internal regulations pursuant to this Standard, those regulations should be publicly distributed.

Standard 25-6.2 Disclosure and dissemination

Law enforcement should not disclose protected records to individuals and entities not involved in the investigation for which they were obtained except in the following circumstances:

(a) Disclosure in the case or cases investigated, pursuant to rules governing investigation, discovery and trial;

(b) Disclosure for purposes of other government investigations, including parallel civil investigations, unless prohibited by law, and except that such disclosure to another government agency should require official certification or, in the case of emergency aid or exigent circumstances, the request of a law enforcement officer or prosecutor;

(c) Disclosure with appropriate redaction for purposes of training, auditing, and other non-investigatory legitimate law enforcement purposes only upon a written determination by a politically accountable law enforcement official that the access is in furtherance of a legitimate law enforcement purpose;

(d) Disclosure of identification records of wanted or dangerous persons and stolen items upon the request of a law enforcement officer or prosecutor; and

(e) Other disclosures only if permitted by statute or upon a finding of a court that the public interest in such disclosure outweighs the privacy of the affected parties.

Part VII. Accountability

Standard 25-7.1 Appropriate sanctions

The legislature should provide accountability for the provisions governing access to and storage and disclosure of records maintained by institutional third parties via appropriate criminal, civil, and/or evidentiary sanctions, and appropriate periodic review and public reporting.

BLACK LETTER WITH COMMENTARY

Part I. Definitions

Standard 25-1.1 Definitions

For purposes of these standards:

(a) "Emergency aid" is government conduct intended to eliminate or mitigate what is reasonably believed to be imminent danger of death or serious physical injury.

Commentary to Standard 25-1.1(a)

All else being equal, preventing crime is always better than punishing it after the fact, and law enforcement officers should be the most free to act when they reasonably believe they are preventing or mitigating imminent death or serious physical injury. Probably for this reason, the Supreme Court has refused to articulate a quantum of suspicion required for emergency aid under the Fourth Amendment, permitting entry to the home upon "an objectively reasonable basis for believing that an occupant is seriously injured or imminently threatened with such injury."[56] No location receives a higher measure of Fourth Amendment protection than the home, both on account of the private things persons do within a home and because entry risks a dangerous physical confrontation.[57] There is no justification for placing greater restriction on emergency aid records access, and thus Standard 25-5.4 permits such access. A reason-

56. Brigham City v. Stuart, 547 U.S. 398, 400 (2006).

57. *See* Kyllo v. United States, 533 U.S. 27, 31 (2001) (acknowledging the home as the "very core" of Fourth Amendment protection); Payton v. New York, 445 U.S. 573, 585 (1980) (recognizing home entry as the "chief evil against which the wording of the Fourth Amendment is directed.").

able belief requires some objective, articulable basis, but it does not rise to the level of probable cause with its "fair probability" standard.[58]

(b) "Exigent circumstances" are circumstances in which there is probable cause to fear imminent destruction of evidence or imminent flight.

Commentary to Standard 25-1.1(b)

As discussed with respect to Standard 25-1.1(a), the home receives the highest, or at least one of the highest, measures of Fourth Amendment protection.[59] Yet law enforcement officers may enter a home without a warrant provided they have both probable cause of criminality and probable cause to fear imminent destruction of evidence or imminent flight.[60] There is no justification for providing greater restriction to records access, and thus Standard 25-5.4 permits such access.

Just as constitutional home entry requires not only a belief about exigency, but also the underlying substantive requirement of probable cause that something inside the home is subject to seizure, these Standards are intended to require the relevant substantive restraint of Standard 25-5.3. The exigency excuses the process ordinarily required (e.g., a court order), but not the quantum of suspicion required (e.g., probable cause).

These Standards use the term "probable cause" as it is defined in the Fourth Amendment context, where the Supreme Court has opined as follows: "Perhaps the best that can be said generally about the required knowledge component of probable cause for a law enforcement officer's evidence search is that it raise a 'fair probability,' or a 'substantial chance,' of discovering evidence of criminal activity."[61] Thus, there must be a "fair probability," or "substantial chance," of imminent destruction of evidence or imminent flight.

---

58. *See* Illinois v. Gates, 462 U.S. 213, 238 (1983) (defining probable cause as "fair probability").

59. A surgical intrusion might require even more scrutiny than a home entry. *See* Winston v. Lee, 470 U.S. 753, 760-62 (1985).

60. *See* Minnesota v. Olson, 495 U.S. 91, 100 (1990) (terming the Minnesota Supreme Court's exigency rule that required probable cause of exigency "essentially the correct standard").

61. Safford Unified School District #1 v. Redding, 557 U.S. 364, 129 S. Ct. 2633, 2639 (2009) (citations omitted).

(c) The "focus of a record" is the person or persons to whom the information in a record principally relates.

Commentary to Standard 25-1.1(c)

When information relating to multiple persons is comingled, typically all those persons are the focus of the record. For example, if a telecommunications provider were to combine the call information of two accounts, those two account holders would both be the focus of that new record. However, it will often be the case that a record principally relating to one individual nonetheless contains information concerning others. The telephone call records of subscriber 'X' might include that X telephoned Y at a certain time, and that X was called by Z at another. Similarly, the bank records of customer X might include that X paid Y a certain amount, and received a certain amount from Z. Nonetheless, those records principally relate only to X, and therefore only X is the focus of those records.

Because this concept is relevant to both consent under Standard 25-5.1 and notice under Standard 25-5.7, the following example will reappear in that respective Commentary: Bob has checking account number 312437 with a bank, and John and Joan Smith have joint checking account number 412835 with the bank. If law enforcement wants to obtain the balance or other account information for account 312437, Bob is the focus of the record. If law enforcement wants to obtain the balance or other account information for account 412835, John and Joan are the focus of the record, even if that information strongly relates to only one of them (e.g., only John has written checks on the account). If law enforcement wants to obtain the account balances for accounts 312437 and 412835 in a single document, Bob, John, and Joan are the focus of the record.

(d) "Law enforcement" means any government officer, agent, or attorney seeking to acquire evidence to be used in the detection, investigation, or prevention of crime.

Commentary to Standard 25-1.1(d)

Subject to the scope limitations of Part II (concerning national security, post-charge discovery, and similar matters), these Standards are meant to broadly apply to criminal justice access.

(e) An "institutional third party" is:

(i) any nongovernmental entity, including one that receives government funding or that acquires information from government sources; and

(ii) any government institution functioning in a comparable capacity, such as a public hospital or a public university.

Commentary to Standard 25-1.1(e)

The acquisition requirements of Part V (Access to Records) apply to law enforcement access to information held by the broad range of nongovernmental third party institutions that might hold information about us, from banks, to hotels, to grocery stores, to data brokers like LexisNexis.[62] So long as they are in part privately owned, they are covered entities. Access to information in law enforcement's own files is also the subject of these standards, but via Part VI (Retention, Maintenance, and Disclosure of Records) rather than Part V. However, where the government provides a service equivalent to private institutions, as in the case of public hospitals and public universities, Part V's restrictions on law enforcement access should apply.

As described in Standard 25-2.1(d), these Standards do not restrict law enforcement efforts to obtain information from an individual not operating as an entity. But *institutional third party* is defined broadly to encompass anyone operating a business, and is therefore not limited to the corporate or other particular business form.

(f) A "politically accountable official" is an upper-level law enforcement official or, in the case of a civil investigation, a civil equivalent, who is either elected or appointed by an elected official, or who is specifically designated for this purpose by an elected or appointed official.

62. *See* LexisNexis Risk Solutions, http://www.lexisnexis.com/risk/ (last visited June 12, 2012).

Commentary to Standard 25-1.1(f)

Because there are more than 17,000 law enforcement entities within the United States[63] and at least as many entities involved in civil enforcement and litigation, it would be impossible to generalize with respect to their command structures. The definition of "politically accountable official" is accordingly broad, but it should be interpreted according to its purpose, which is to require action by an individual who is politically accountable. Upon such political accountability, law enforcement can access appropriately inclusive bodies of de-identified records (see Standard 25-5.6), can access records held by a different government agency (see Standard 25-6.2(b)), and can disclose records for training and other non-investigatory legitimate law enforcement purposes (see Standard 6.2(c)).

(g) A "record" contains information, whether maintained in paper, electronic, or other form, that is linked, or is linkable through reasonable efforts, to an identifiable person. A "de-identified record" contains information that is not so linkable.

Commentary to Standard 25-1.1(g)

There is an important emerging body of computer science and legal literature that questions the concept of de-identification. If information is to retain utility, it is, given the requisite outside data, possible to re-identify that information.[64] In other words, "data can be either useful or perfectly anonymous but never both."[65]

A simple example helps to make the point, albeit not constituting anything like a scientific proof. Assume a database of hospital admissions that includes patient information (name, address, birth date, sex), health condition information (reason for admission, basic vital statistics), and

63. U.S. Bureau of Justice Statistics, *Census of State and Local Law Enforcement Agencies, 2004*, http://www.census.gov/compendia/statab/2010/tables/10s0333.pdf (last visited June 12, 2012).

64. *See generally* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701 (2010).

65. *Id*. at 1704. *See also* Arvind Narayanan & Vitaly Shmatikov, *Privacy and Security: Myths and Fallacies of "Personally Identifiable Information"*, 53 Communications of the ACM 6, 24 (June 2010). *Cf.* Felix T. Wu, *Privacy and Utility in Data Sets*, U. Colo. L. Rev. (forthcoming 2013) (urging a more moderate view).

attendant circumstances (date and time). One means of "de-identification" would be to remove the patient names and street addresses (retaining the ZIP code), and make the resulting database publicly available to benefit those researching health trends. But this would be very poor de-identification, because the combination of ZIP code, birth date, and sex uniquely identifies somewhere between 61 to 87% of the American population.[66] In retrospect, this is not surprising, as a ZIP code might contain on the order of 8,000 persons of a given sex,[67] and the birth date (including year) does the rest. A better de-identification would be to remove all address information, but notice that the database has just become less useful: those tracking medical trends now have less precise geography. A still better de-identification would be to remove birth date as well; once again those tracking medical trends have lost some utility. Furthermore, the scientific claim is that it is nonetheless still possible to re-identify the data, albeit probably not as easily as before. But even that is hard to know for sure: imagine if the hospital had high-resolution surveillance cameras at its entrance, and their recordings were retained. Somebody having access to that data, as well as to, say, driver's license photographs, might be able to make re-identifications.

All of this is of great concern where allegedly de-identified data is going to be released to the public, for it is impossible to know who will seek to re-identify it, what data they will have available in that attempt, and what they will do with the data if successfully re-identified. Therefore, it is clear that de-identification is not the panacea it might have once seemed, and lawmakers addressing it in its broader context will have to decide whether there are definable modes of de-identification that are nonetheless worthwhile, whether to separately criminalize re-identification of de-identified data sets, and a host of other complicated issues.[68]

---

66. *See id.* at 1705. *See also* Gina Kolata, *Online Hunt for DNA Sequences Leaves Privacy Compromised*, N.Y. Times, Jan. 18, 2013, at A15.

67. For example, the zip code 01776, selected solely for its Revolutionary War significance, contained 17,659 people according to the 2010 census, with essentially equal numbers of men and women. U.S. Census Bureau FactFinder, http://factfinder2.census.gov/faces/tableservices/jsf/pages/productview.xhtml?pid=DEC_10_SF1_GCTP2.ST09&prodType=table (last visited June 12, 2012).

68. *See, e.g.*, Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. Rev. 1814, 1877-78 (2011) (proposing a three-tiered system of (1) identified material or that with a substantial risk of re-identification ("identified"); (2) material with a low to moderate risk of re-identification ("identifiable");

Fortunately, the purpose of de-identification in these Standards is more narrow. Pursuant to Standard 25-5.6, the data at issue are not being released to the public, but rather only to law enforcement in furtherance of a legitimate law enforcement purpose, and subject to the other constraints of Parts V, VI, and VII. Those potentially include, for example, administrative, civil, and/or criminal liability for their breach. Therefore, while lawmakers should be aware of developments in the science and law of de-identification, the concept retains utility.[69] Whether or not it is possible for useful data to be *perfectly* anonymous, de-identification can avoid unintended and unsophisticated illegitimate identifications.[70]

Thus, the Standards consider data to be identified if it is "linkable through reasonable efforts to an identifiable person," where "reasonable" is intended to be sufficiently flexible to accommodate both (1) developments in the science of de-identification and re-identification, and (2) limited government resources, in that de-identification is not meant to itself present an insurmountable hurdle to access, given that it provides only one safeguard in a system of safeguards.[71] If, however, it comes to be the case that a legislature considers sophisticated de-identification an entirely futile exercise, then it could decide to instead require that a few explicit identifiers be removed (e.g., name, social security number, and street address), and rely entirely on the remaining restraints of Parts

---

and (3) material with a remote risk of re-identification ("non-identifiable")); UK Information Commissioner's Office, *Anonymisation: Managing Data Protection Risk Code of Practice* (Nov. 20 2012), http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/anonymisation_code.ashx (describing the benefits and difficulties of anonymization).

69. The Federal Trade Commission found ample assurance in reasonable de-identification backed by the sanctions of laws punishing deceptive trade practices. *See* Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change* iv, 18-22 (March 2012), available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf (last visited June 12, 2012).

70. For a description of de-identification, and how it differs from anonymization, see NIST Special Publication 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* 4-4 to 4-6 (April 2010), available at http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf (last visited June 12, 2012).

71. The Federal Trade Commission similarly requires that data be "not reasonably identifiable." *See Protecting Consumer Privacy*, *supra* note 69, at 22.

V, VI, and VII.[72] Or, it could instead require another mode of selective revelation before permitting Standard 25-5.6 disclosures.[73]

72. *See* Commentary to Standard 25-5.6, *infra* p. 111.
73. *See id.*

Part II. Scope

Standard 25-2.1 Scope

These standards relate to law enforcement investigatory access to, and storage and disclosure of, records maintained by institutional third parties. These standards do not relate to:

(a) access to records for purposes of national security;

Commentary to Standard 25-2.1(a)

These Standards do not relate to records access for purposes of national security. Records access can be critical in keeping our country safe from foreign attack, as evidenced by the fact that various data concerning the plot of the September 11, 2001 terrorists was stored by institutional third parties.[74] But such access could be abused, even if well intentioned, as fear is a strong motivator to abandon the principles upon which our democracy depends, and ex-post "dot connecting" is far easier and more defined than prediction.[75] Future revisions or other task forces might therefore want to take up this topic, but for reasons of economy and precision these Standards do not relate to national security acquisitions, meaning those intended to acquire information con-

74. *See* 9/11 Commission Report, available at http://www.911commission.gov/report/911Report.pdf and http://www.gpo.gov/fdsys/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf (last visited June 13, 2012).

75. *See, e.g.*, Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters* (March 2007), available at http://www.justice.gov/oig/special/s0703b/final.pdf (last visited June 13, 2012); Office of the Inspector General, *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006* (March 2008), available at http://www.justice.gov/oig/special/s0803b/final.pdf (last visited June 13, 2012); Charles Doyle, *National Security Letters in Foreign Intelligence Investigations: Legal Background and Recent Amendments*, Congressional Research Service Report RL33320 (Sept. 8, 2009), available at http://www.fas.org/sgp/crs/intel/RL33320.pdf (last visited June 13, 2012).

cerning a foreign power or an agent thereof.[76] This would include not only information directly relating to such a foreign agent, but information relevant to a legitimate investigation of the agent.[77] If information is lawfully gathered for that national security purpose, these Standards do not address its use in a criminal investigation.

(b) access to records after the initiation and in the course of a criminal prosecution;

Commentary to Standard 25-2.1(b)

These Standards do not relate to records access in the course of a criminal prosecution. In other words, these Standards apply to the investigatory phase of criminal procedure, and not to the adjudicatory phase, where the two are separated by the Sixth Amendment's trigger: "the initiation of adversary judicial criminal proceedings—whether by way of formal charge, preliminary hearing, indictment, information, or arraignment."[78]

---

76. Previous ABA Standards have made a similar decision. *See, e.g.,* ABA Standards for Criminal Justice, *Electronic Surveillance, Section A: Electronic Surveillance of Private Communications* 5-6 (3d ed. 2001). Both constitutional and statutory law differs for national security investigations. *See, e.g.,* United States v. United States District Court (aka "the Keith case"), 407 U.S. 297 (1972) (distinguishing ordinary crime, domestic security threats, and foreign security threats); 50 USC §§ 1801-1812 (the Foreign Intelligence Surveillance Act).

77. Prior to passage of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (the "Patriot Act"), the statutory national security carve-out was limited to information pertaining to a foreign power or an agent of a foreign power. *See, e.g.,* 18 U.S.C. § 2709(b)(1)(B) (effective October 21, 1986 to October 25, 2001) (permitting access to certain telephone records). Today, according to section 505 of the Patriot Act, the carve-out is more generous, in that the information must be "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States." 18 U.S.C. § 2709(b)(1). In other words, the national security carve-out now includes telephone records of a person who is *not* an agent of a foreign power so long as those records are relevant to a national security investigation of such a person.

78. Moore v. Illinois, 434 U.S. 220, 226 (1977) (quoting Kirby v. Illinois, 406 U.S. 682, 689 (1972)). The Sixth Amendment provides that "In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been

There are of course privacy concerns in prosecution access. For example, the Federal Rules of Criminal Procedure typically require notice and an opportunity to be heard before third party records pertaining to a victim can be accessed.[79] But these matters are beyond the scope of these Standards. Not only might the substantive interests be different (for example, such a trial subpoena may be seeking information going to the credibility of a witness rather than to criminality), but once adversary judicial proceedings have commenced, a defendant enjoys the Sixth Amendment guarantee to counsel and other guarantees of judicial oversight that do not exist during the investigatory phase.

(c) access to records via a grand jury subpoena, or in jurisdictions where grand juries are typically not used, a functionally equivalent prosecutorial subpoena;

Commentary to Standard 25-2.1(c)

The federal government and some states have a long history of vesting broad investigatory powers in citizen grand juries. In the words of the United States Supreme Court,

> The grand jury occupies a unique role in our criminal justice system. . . . [T]he grand jury can investigate merely on suspicion that the law is being violated, or even just because it wants assurance that it is not. . . . As a necessary consequence of its investigatory function, the grand jury paints with a broad brush. A grand jury investigation is not fully carried out until every available clue has been run down and all witnesses examined in every proper way to find if a crime has been committed."[80]

Although the investigatory powers of a federal grand jury "are nevertheless not unlimited,"[81] "a grand jury subpoena issued through nor-

previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defence." U.S. Const. amend. VI.

79. Fed. R. Crim. P. 17(c)(3).

80. United States v. R. Enterprises, Inc., 498 U.S. 292, 297 (1991) (internal quotation marks omitted).

81. *Id.* at 299.

mal channels is presumed to be reasonable,"[82] and a request is legally obligatory unless "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation."[83] This is the most minimal level of relevance required by the criminal law.

This very significant investigatory authority has been thought justified by history, by the public's "right to every man's evidence,"[84] by strict secrecy provisions, and by court supervision.[85] But it has also been subject to critical questioning. When federal grand juries return "true bills" 99.6% of the time,[86] and are not meaningfully involved in the issuance of most subpoenas,[87] one can question whether grand jury subpoena authority should be given the "pass" it has historically received. Some have questioned whether the Supreme Court precedents, which were issued in the context of a grand jury accessing records pertaining to a business, should apply when personal records are at issue.[88] There was robust debate on these topics during the drafting of these Standards.

Ultimately, however, these Standards are in accordance with the historic treatment, including acknowledging a longstanding alternative in some jurisdictions where grand juries are typically not used. Legislatures, courts, and administrative agencies should be careful, however, to strictly cabin this exception to means for which (1) there is historical practice that has not been discredited and that remains relevantly applicable, and (2) that historical practice includes privacy safeguards equivalent to those of the federal grand jury.

(d) access to records from an individual not acting as an institutional third party;

82. *Id.* at 301.

83. *Id.* at 301.

84. Branzburg v. Hayes, 408 U.S. 665, 688 (1972).

85. *See id.*; Fed. R. Crim. P. 6(e).

86. *See* Andrew D. Leipold, *Why Grand Juries Do Not (And Cannot) Protect the Accused*, 80 Cornell L. Rev. 260, 274 (1995) (arguing, however, that these statistics do not tell the whole story).

87. *See* Doe v. DiGenova, 779 F.2d 74, 80 (D.C. Cir. 1985) ("Nor does the grand jury necessarily approve or even have knowledge of a subpoena prior to its issuance."); Leipold, *supra* note 86 at 314-17.

88. *See* Christopher Slobogin, Privacy at Risk: The New Government Surveillance and the Fourth Amendment 139-67 (University of Chicago Press 2007).

Commentary to Standard 25-2.1(d)

These Standards apply to law enforcement access to records held by the broad range of third party institutions that might hold information about us, from banks, to hotels, to grocery stores, to data brokers like LexisNexis.[89] The Standards do not restrict access to records from an individual not acting as a business entity, for two reasons.

First, an individual has an autonomy and free speech interest in choosing to share information that will often trump any privacy interest.[90] That is, the right of the purveyor of information to control its dissemination and use (see Commentary to Standard 25-3.3) is in significant tension with the freedom of the individual who receives the information to speak his or her mind.[91] Institutional third parties may also have some First Amendment rights,[92] but these Standards assume that the balance in cases involving institutional record-holders is different than when the autonomy and freedom of expression of an individual not acting as a business entity are at stake.

Second, the motivating concern of these Standards is the much more significant threat to privacy in the ever-increasing amounts of information contained within systems of records maintained by entities. Therefore, if law enforcement wishes to read a personal letter sent to a friend, and seeks the letter from that friend, these Standards do not apply.

Finally, these Standards relate to access to *records*, not inquiry into personal recollection.[93] If law enforcement wants to question a doctor

89. *See* LexisNexis Risk Solutions, http://www.lexisnexis.com/risk/ (last visited June 12, 2012).

90. *See* Christopher Slobogin, *Transaction Surveillance by the Government*, 75 Miss. L.J. 139, 185-86 (2005). There is a special case when law enforcement requests information directly from a target, which has been the subject of discussion and constitutional controversy at least since the 1886 decision in *Boyd v. United States*, 116 U.S. 616 (1886), with the Court more recently returning to the topic in *United States v. Hubbell*, 530 U.S. 27 (2000). *See* Slobogin, Privacy at Risk, *supra* note 88.

91. *See* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 Stan. L. Rev. 1049 (2000).

92. S*ee* Citizens United v. Federal Election Commission, 558 U.S. 310, 130 S. Ct. 876 (2010) (holding that a federal statute barring independent corporate expenditures for electioneering communications violated the First Amendment).

93. Thus, every Standard references access to *records*. *See, e.g.*, Standards 25-5.1 through 25-5.4.

regarding his or her personal recollection of a patient, these Standards are not implicated. But if that doctor were to read records to law enforcement, or if law enforcement wants to itself read those records, then law enforcement should be required to comply with these Standards.

(e) acquisition of information contemporaneous with its generation or transmission;

Commentary to Standard 25-2.1(e)

Forty years ago, the ABA promulgated its Standards relating to Electronic Surveillance, providing detailed guidelines for the interception of the contents of private communications.[94] Now in its Third Edition,[95] those Standards guide access to telephone, e-mail, and oral communications legally governed by the federal Wiretap Act,[96] the federal Stored Communications Act,[97] and related state laws. More recently, in 1999, the ABA promulgated a "Section B" relating to Technologically-Assisted Physical Surveillance.[98] Those Standards guide law enforcement physical surveillance that is technologically enhanced, divided into the four categories of video surveillance, tracking devices, illumination and telescopic devices, and detection devices.

These current Standards are not meant to duplicate or supplant either of those predecessors, and therefore relate only to law enforcement access to existing records, what some term "historical" surveillance as opposed to "prospective" surveillance. Thus, there remains a gap insofar as no standards have been promulgated relating to the interception of non-content (transactional) information relating to communications, such as via pen registers and trap and trace devices.[99] Although such surveillance has some relation to the current project, in that presumably the same standard should typically apply whether information is being

94. ABA Standards for Criminal Justice, Electronic Surveillance (1st ed. 1971).

95. ABA Standards for Criminal Justice, Electronic Surveillance, Section A: Electronic Surveillance of Private Communications (3d ed. 2001).

96. 18 U.S.C. §§ 2510-2522.

97. 18 U.S.C. §§ 2701-2712.

98. ABA Standards for Criminal Justice, Electronic Surveillance, Section B: Technologically-Assisted Physical Surveillance (1999).

99. *See* ABA Standards for Criminal Justice, Electronic Surveillance, Section A, *supra* note 95 at 6-7.

obtained in real-time or historically,[100] it seems most appropriate that real-time surveillance remain the province of those other Standards. The one area of overlap is law enforcement access to existing communications records, because that is one particular subset of law enforcement access to third party records.

(f) an institutional third party:

(i) that is a victim of crime disclosing information that is evidence of that crime or that is otherwise intended to protect its rights or property; or

Commentary to Standard 25-2.1(f)(i)

When an institutional third party conveys information to law enforcement because it is itself a victim of crime, even upon the government's request, the primary motivation is not to assist law enforcement but instead to obtain redress or to protect against further harm.[101] Thus, for example, the federal electronic communications laws permit service provider acquisitions and disclosures that are intended to protect their rights and property,[102] and these Standards do the same.

(ii) deciding of its own initiative and volition to provide information to law enforcement.

---

100. Existing statutory regimes sometimes do differentiate between real-time and historical surveillance. For example, to acquire electronic mail in real time, the government must obtain a Title III "super warrant." *See* 18 U.S.C. § 2510(12) (defining "electronic communication"); 18 U.S.C. §§ 2511, 2516, 2518 (articulating requirements). But to obtain historic electronic mail from an internet service provider, the government must obtain, at most, a search warrant. *See* 18 U.S.C. § 2703(a). This is not typically a logical distinction, as the privacy intrusion is identical in either case. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 282-88 (6th Cir. 2010) (striking down a provision of the Stored Communications Act that permits law enforcement access to historic electronic mail without a warrant); In re Application of the United States for Historic Cell Site Data, 747 F. Supp. 2d 827, 839 (S.D. Tex. 2010) ("The . . . distinction between prospective and historical location tracking is not compelling, because the degree of invasiveness is the same, whether the tracking covers the previous 60 days or the next."). Of course, if different information would be available, that might be good reason for a different standard. In any event, these will be considerations for future revisions of other Standards.

101. *See* Burrows v. Superior Court, 529 P.2d 590, 594 (Cal. 1974) (recognizing victim exception to constitutional restriction on transfer).

102. *See* 18 U.S.C. § 2511(2)(a)(i) (provider exception for acquisitions contemporaneous with transmission); 18 U.S.C. § 2702(b)(5) (provider exception for stored communications).

Commentary to Standard 25-2.1(f)(ii)

These Standards do not restrict purely private conduct, even when it results in information being disclosed to law enforcement. Thus, if an institutional third party decides entirely upon its own initiative to voluntarily convey information to law enforcement, nothing in these Standards relates to that transfer.

In this sense, these Standards are less comprehensive than existing laws that do restrict private disclosures, such as the federal Stored Communications Act[103] and the Right to Financial Privacy Act.[104] Private data acquisition and disclosure presents benefits, risks, and harms that are in some ways similar to, but not identical to, those raised by law enforcement access. The Standards therefore do not imply that such restrictions are unwise or unnecessary, and those laws are obviously controlling where in effect. Rather, the Standards merely recognize the inherent subject matter limitation of criminal justice standards, and also acknowledge these distinctions raised by the Department of Defense Technology and Privacy Advisory Committee ("TAPAC") in the context of data mining:

> [D]ata mining by the government presents privacy issues different from—and often greater than—data mining by private entities, and therefore warrants special scrutiny. This focus on government activity reflects the reality that only the government exercises the power to compel disclosure of information and to impose civil and criminal penalties for noncompliance. Only the government collects and uses information free from market competition and consumer preferences. When dealing with the government, individuals have no opportunity to express their expectations of privacy by choosing to do business elsewhere or by not engaging in transactions at all. We, like the framers of our Constitution, recognize that in the

103. *See* 18 U.S.C. §§ 2702(b)(1) to 2702(b)(8) (permitting a public provider to voluntarily disclose communications when, inter alia, evidence of crime is inadvertently obtained or upon danger of death or serious physical injury that requires disclosure without delay).

104. *See* 12 U.S.C. § 3402 (prohibiting bank disclosure without requisite process).

> government context, the law alone provides—or should provide—protection for those expectations.[105]

So regulation of private access and disclosure is a worthy topic in its own right, but it is a different topic and not one within the scope of these Standards.

Further, if a law enforcement official makes a generalized plea that citizens come forward with any relevant information, including perhaps offering a reward for such assistance, a subsequent decision by an institutional third party to provide information remains of its own initiative and volition.[106] This is true whether the plea relates to a specific investigation or incident or more generally requests information on anything deemed "suspicious."[107]

The situation is markedly different, however, when law enforcement initiates a specific contact with a particular third party, and that contact leads to a records transfer. Just as a private person is treated as an agent of the government for Fourth Amendment[108] or Sixth Amendment

---

105. TAPAC, *Safeguarding Privacy in the Fight Against Terrorism* 24 (2004), available at http://www.defenselink.mil/news/Jan2006/d20060208tapac.pdf (last visited June 13, 2012). Similarly, Professor Jed Rubenfeld has recognized that

> the government's law enforcement power is unique. . . . The ability of government to intrude, monitor, punish, and regulate is greater than that of private actors by many orders of magnitude. But more than this, the state has a right and duty to intrude into people's lives that private parties do not. As the nation's principal law enforcer, the state can and should take actions with respect to private property that would constitute trespass or theft if done by private parties. Policemen can and should enter homes when no sensible person or reasonable stranger would. But precisely because the state's law enforcement power gives it a license to intrude into our homes and lives in ways that private parties cannot, the state poses dangers to a free citizenry that private parties do not.

Jed Rubenfeld, *The End of Privacy*, 61 Stan. L. Rev. 101, 118 (2008).

106. *See, e.g.*, United States v. Valen, 479 F.2d 467, 469-70 (3d Cir. 1973) (holding in the Fourth Amendment context that a generalized plea that one notify officials if he were to come across anything suspicious in the future and the subsequent paying of a reward did not transform a private actor into a government actor).

107. *See, e.g.*, Bertolotti v. State, 476 So.2d 130, 132 (Fla. 1985) (holding in the Fourth Amendment context that "[a] community-wide, regularly advertised program which rewards any citizen who provides information useful to the police in their criminal investigations is not tantamount to recruiting police agents").

108. *See* United States v. Souza, 223 F.3d 1197, 1201 (10th Cir. 2000) ("In determining whether a search by a private person becomes a government search, the following two-

purposes,[109] so an institutional third party transferring information after being contacted by law enforcement is treated as a government actor, such that the acquisition is one to which these Standards relate. It is the position of these Standards that there is no benefit to creating a complicated jurisprudence that might exempt a few such transfers on particular facts. Therefore, if law enforcement initiates the contact leading to a records transfer, whether it be a particular request or a generalized desire for access to the third party's records, that transfer is one to which these Standards should relate unless the third party is a victim according to Standard 25-2.1(f)(i).

Standard 25-2.2 Constitutional floor

A legislature or administrative agency may not authorize a protection less than that required by the federal Constitution, nor less than that required by its respective state Constitution.

Commentary to Standard 25-2.2

This Standard articulates two bedrock principles of American constitutional law: neither a legislature nor an administrative agency may infringe those rights guaranteed by the federal Constitution, and neither a state legislature nor a state agency may infringe those rights guaranteed by its respective state Constitution. Although a legislature or agency can disagree with a court regarding how *private* is given information, it cannot deviate from a constitutional standard of protection. Because these propositions are not subject to debate, this Standard departs from the typical aspirational language of standards (i.e., it employs the construction "may not" rather than "should not").

part inquiry is utilized: 1) whether the government knew of and acquiesced in the intrusive conduct, and 2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends.") (internal quotation marks omitted).

109. *See* Ayers v. Hudson, 623 F.3d 301, 310-12 (6th Cir. 2010) (describing tests in various circuits).

Part III. General Principles

Standard 25-3.1 Records available

Institutional third parties maintain records ranging from the most mundane to those chronicling the most personal aspects of people's lives, and when those records are stored digitally, access and distribution costs are diminished. These records include such things as the content of communications; medical diagnoses, treatments, and conditions; internet browsings; financial transactions; physical locations; bookstore and library purchases, loans, and browsings; other store purchases and browsings; and media viewing preferences.

Commentary to Standard 25-3.1

With the maturation of digital storage and search technologies, and virtually costless distributions, we now live in a world of ubiquitous third party information. Although data can of course be scrubbed and is routinely overwritten, it is nonetheless difficult to overstate the magnitude of information that now resides with third parties, from our shopping preferences (residing with our credit and debit card providers and individual stores), to our communications (residing with our service providers and other intermediaries), to our health information (residing with doctors, pharmacies, hospitals, and insurance companies), to our viewing habits (residing with our cable and internet providers), to our very location (residing with our mobile phone providers and toll tag operators).

In the words of Judge Richard Posner,

> [A] person would have to be a hermit to be able to function in our society without voluntarily disclosing a vast amount of personal information to a vast array of public and private demanders. This has long been true, but until quite recently the information that people voluntarily disclosed to vendors, licensing bureaus, hospitals, public libraries, and so forth, was scattered, fugitive (because the bulki-

> ness of paper records usually causes them to be discarded as soon as they lose their value to the enterprise), and searchable only with great difficulty. So although one had voluntarily disclosed private information on innumerable occasions to sundry recipients, one retained as a practical matter a great deal of privacy. But with digitization, not only can recorded information be retained indefinitely at little cost, but also the information held by different merchants, insurers, and government agencies can readily be pooled, opening the way to assembling all the recorded information concerning an individual in a single digital file that can easily be retrieved and searched.[110]

Moreover, whole categories of data are stored that never were before. Not long ago, if a customer made a purchase with cash, a bookstore often would have made no individualized record of what was bought. Similarly, a library would have recorded only the materials ultimately checked out. But when we browse online, including bookstores and libraries, multiple service providers might record every article, picture, book and video that we peruse. Whereas in a store purchase in an earlier day a clerk might recognize or remember a face and some of the items purchased, today when we purchase with "discount" or "customer loyalty" cards, the store records everything purchased, no matter the location or time of sale. If we purchase online, the store might record everything we even consider purchasing and store this information for as long as it is considered financially or legally beneficial. For many of us, credit and/or debit cards provide a virtual dossier of our daily activities. Whereas the motor vehicle department would have known only our basic physical characteristics and those of our vehicle, today via traffic cameras, electronic toll tags, cell tower triangulation, and GPS-enabled cell phones offering mobile commerce and direction services, entities record our travels. Whereas one used to anonymously pick up the broadcast television signal with an antenna, today our provider often knows what we watch and when, as does our provider of video rentals. At one time our telephone provider created a log of our long distance calls; today it might make a record of all of our calls and our physical location. Whereas we used to store computer files on

110. Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. Chi. L. Rev. 245, 248 (2008).

our home computers, today for reasons of geographic flexibility in data access and robust backup, many now store them instead on third party servers, taking advantage of so-called "cloud computing." Entire business models depend upon the value of provided information, providing "free" services online that are entirely subsidized by the value of the personal information they collect.[111] Finally, as Judge Posner noted, data aggregators can combine data from these disparate sources of information into single locations.

There is of course some limitation on the amount of data that can be stored, but we are all aware of vastly increasing storage capacities. A few years ago we typically contented ourselves with so-called 1.44 megabyte "floppies," meaning each could hold approximately 1,500,000 bytes of data. Today a blu-ray disc accommodates 50 gigabytes (roughly 50,000,000,000 bytes), storing the equivalent of over 35,000 such floppies, and portable terabyte hard drives are cheaply available that each store roughly 1,000,000,000,000 bytes of data, the equivalent of 700,000 such floppies.

It is not merely the amount of data that has changed, but also its nature. When records were stored in paper form, it required effort to move through those stacks and find relevant information. But when data is stored digitally, after an initial investment in architecture searching is easy and essentially costless. And whereas paper records required potentially costly distribution in the form of photocopying and mailing or courier fees, digital records can be costlessly distributed via the Internet and other networks.

Technology can of course increase privacy. After all, at one time it was difficult to communicate securely without meeting face to face. But it has also contributed to the phenomenon that far more information about our lives is recorded and stored than ever before, most of it in a digital format that can be searched and electronically distributed. And these trends—increasing data collection and storage, cheap and effective searching, and cheap distribution—show no signs of slowing.

---

111. The social networking site Facebook is approaching a billion customers with just such a business model, and raised $16 billion in the third-largest public offering in United States history. *See The Value of Friendship*, The Economist, Feb. 4, 2012, at 23; Evelyn M. Rusli & Peter Eavis, *Facebook Raises $16 Billion in I.P.O.*, N.Y. Times DealBook, May 17, 2012, available at http://dealbook.nytimes.com/2012/05/17/facebook-raises-16-billion-in-i-p-o/ (last visited June 13, 2012).

Standard 25-3.2 Need for records access

Obtaining records maintained by institutional third parties can facilitate, and indeed be essential to, the detection, investigation, prevention and deterrence of crime; the safety of citizens and law enforcement officers; and the apprehension and prosecution of criminals; and can be the least confrontational means of obtaining needed evidence.

Commentary to Standard 25-3.2

In terms of their number, "records searches"—in which law enforcement obtains evidence of crime via records maintained by institutional third parties—are surely one of the most important investigatory activities, and have been for many years. Access to such records deters and detects crimes as diverse as kidnapping (phone records), public corruption and organized crime (bank records), and child sexual assault (internet records). Even a seemingly "routine" street crime might depend upon records access for resolution, as when hospital admission records allow police to discover who might have been involved in a recent shooting, or when toll tag records allow police to learn the culprit in a fatal hit-and-run. In planned crimes, internet service provider records might demonstrate that planning or motive. Thus, in the Illinois first-degree murder case of *People v. Zirko*, relevant internet searches by Zirko included "hire a hitman," demonstrated an interest in gun shows, and mapped the route from Zirko's house to the victim's.[112]

Moreover, records access permits law enforcement to deter or punish private access that is itself harmful and criminal, such as identity theft and computer hacking. As a Chicago policeman has aptly noted, "No other section of the population avail themselves more readily and speedily of the latest triumphs of science than the criminal class."[113] Only this statement was made in 1888, speaking of the electric telegraph, demonstrating that the more things change, in this sense the more they remain the same.

112. 976 N.E.2d 361, 373, 377 (Ill. App. 2012). *See also* State v. McGuire, 16 A.3d 411, 423-24 (N.J. Super. 2011) (involving similarly relevant search terms). Although in these cases the search history appears to have resided on the perpetrator's computer, those terms might also be recoverable from the third party provider.

113. *Dusting for Digital Fingerprints*, The Economist, March 12, 2005, at 79.

When evidence is available via third party records, records access has the additional benefit of not risking a physical confrontation with the target. When police enter a home or otherwise seek to forcibly obtain information directly from a suspect, there is always a threat of violence and therefore of harm either to the police, to bystanders, or to the suspect him- or herself. The ability to obtain evidence from a neutral third party eliminates this risk. Similarly, while a prosecutor might subpoena records from a suspect, that risks their destruction despite the threat of criminal liability for obstruction. Once again, third party records access largely eliminates that risk.

It should be noted that while deterrence is appropriately mentioned as a benefit of records access, the Standards do not mean to authorize law enforcement access to records for the *purpose* of deterrence (e.g., obtaining and searching through records in order to create a societal perception of being watched). Rather, deterrence is a secondary effect of law enforcement investigating crime.

Standard 25-3.3 Implications of records access

Law enforcement acquisition of records maintained by institutional third parties can infringe the privacy of those whose information is contained in the records; chill freedoms of speech, association, and commerce; and deter individuals from seeking medical, emotional, physical or other assistance for themselves or others.

Commentary to Standard 25-3.3

Unlike the goals and benefits of law enforcement, those of privacy can be difficult to articulate.[114] But they are no less real, and from its founding America has respected them. Studies by Alan Westin have confirmed a relationship between political philosophy and privacy throughout

114. *See generally* Philosophical Dimensions of Privacy: An Anthology (Ferdinand David Schoeman ed., Cambridge University Press 1984); Daniel J. Solove et al., Privacy, Information, and Technology 35-36 (Aspen Publishers 2006); Daniel J. Solove, *Conceptualizing Privacy*, 90 Cal. L. Rev. 1087 (2002); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477 (2006).

Western civilization,[115] but he identifies the American Republic of 1790-1820 as "the first 'modern' privacy system":

> Of course, the word 'privacy' does not appear in the U.S. Constitution or the Bill of Rights. However, the Founding Fathers gave the American Republic all the key components of a broad-scale privacy regime—fundamental constitutional guarantees against unreasonable search and seizure; rejection of compulsory testimony and self-incrimination; and privacy for association and religion in the First Amendment. Privacy rights in first-class mail and in Census enumeration were written into early federal legislation or regulation, and the privacy of letters was given judicial protection against private publication against the wishes of the writer or recipient. And, by rejecting internal government passports, elaborate government record-keeping, government spy networks, and other apparatuses of late 18th and early 19th century royal surveillance, the American republic nurtured socio-political traditions of individual autonomy and non-surveillance that gave daily vitality to the early constitutional and legal rules.[116]

The First Amendment's freedom of speech also sometimes protects privacy in the form of anonymous speech,[117] and the Supreme Court has interpreted the Bill of Rights to include substantive due process that protects private decisions.[118] Thus, privacy is a critical component of many fundamental rights,[119] as described more fully in the Commentary

115. *See* Alan F. Westin, Historical Perspectives on Privacy: From the Hebrews and Greeks to the American Republic 4-5, 9 (presented and distributed at the 2009 Privacy Law Scholars Conference, and quoted with permission).

116. *Id.* at 9-10.

117. *See* McIntyre v. Ohio Election Comm'n, 514 U.S. 334, 342 (1995).

118. *E.g.*, Griswold v. Connecticut, 381 U.S. 479, 485-86 (1965) (recognizing marital privacy); Whalen v. Roe, 429 U.S. 589, 599 (1977) (recognizing information privacy).

119. In the words of scholar Benjamin Goold,

> It is hard to imagine, for example, being able to enjoy freedom of expression, freedom of association, or freedom of religion without an accompanying right to privacy. Indeed, one of the greatest dangers of unfettered mass surveillance is the potential chilling effect on political discourse, and on the ability of groups to express their views through protest and other forms of peaceful civil action.

to Standard 25-4.1(a). Independently, a number of state constitutions explicitly protect privacy,[120] and privacy law has not been stagnant, but instead in every category has adapted to the changing circumstances of over two hundred years.

At privacy's core—at least at the core of the information privacy that is at issue in these Standards—is an ability to control what information about you is conveyed to others, and for what purposes.[121] In the words of scholar Benjamin Goold,

> Although it is possible to talk of privacy as simply the right to be 'let alone', its status as a right derives primarily from its relationship to ideas of autonomy and self-determination. Privacy is valuable because it is necessary
>
> By ensuring that there is a limit on what the state can reasonably expect to know about us, privacy not only helps to protect individual autonomy, but also ensures that we are free to use that autonomy in the exercise of other fundamental rights.

Benjamin J. Goold, *Surveillance and the Political Value of Privacy*, 1 Amsterdam L. Forum 3, 4-5 (2009).

120. *See* Alaska Const. art. I, § 22; Ariz. Const. art. II, § 8; Cal. Const. art I, § 1; Fla. Const. art. I, § 23; Haw. Const. art. I, § 6; Ill. Const. art I, § 6; La. Const. art. I, § 5; Mont. Const. art. II, § 10; S.C. Const. art. I, § 10; Wash. Const. art. I, § 7.

121. Alan Westin's seminal 1967 work stated this principle as follows: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Alan F. Westin, Privacy and Freedom 7 (1967). *See* Shaktman v. State, 553 So.2d 148, 150 (Fla. 1989) (adopting this definition). More recently Westin writes that "[m]ost definitions of privacy agree on a core concept: that privacy is the claim of an individual to determine what information about himself or herself should be known to others. This also involves when such information will be communicated or obtained and what uses will be made of it by others." Westin, *Historical Perspectives*, *supra* note 115 at 4.

To Charles Fried, "[P]rivacy [i]s that aspect of social order by which persons control access to information about themselves." Charles Fried, *Privacy*, 77 Yale L. J. 475, 493 (1968). One of the key themes in Samuel Warren and Louis Brandeis's seminal 1890 article was each individual's "right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others." Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 198 (1890). Andrew Taslitz has explained why this control matters: "Each of us wears many masks wherein each mask reflects a different aspect of who we really are. . . . [W]e want to choose the masks that we show to others; any such loss of choice is painful, amounting almost to a physical violation of the self. When we are secretly watched, or when information that we choose to reveal to one audience is instead exposed to another, we lose that sense of choice." Andrew E. Taslitz, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions*, 65 Law & Contemp. Probs. 125, 131 (2002).

> for the proper development of the self, the establishment and control of personal identity, and the maintenance of individual dignity. Without privacy, it not only becomes harder to form valuable social relationships—relationships based on exclusivity, intimacy, and the sharing of personal information—but also to maintain a variety of social roles and identities. Privacy deserves to be protected as a right because we need it in order to live rich, fulfilling lives, lives where we can simultaneously play the role of friend, colleague, parent and citizen without having the boundaries between these different and often conflicting identities breached without our consent.[122]

Quite clearly law enforcement access to records can therefore infringe upon privacy, albeit often being necessary.[123]

Privacy is not extinguished by the sharing of information with select others, as privacy is not an indivisible commodity limited to secrecy. Intimacy too is a core construct, whether the revelations be personal ones intended to "share sensitive ideas and emotions, receive help and feedback, and deepen bonds of mutual self-revelation and connection,"[124] or business revelations intended to permit the daily commerce of modern life.[125]

122. Benjamin Goold, *Surveillance and the Political Value of Privacy*, 1 Amsterdam L. Forum 3, 3-4 (2009).

123. For a more complete exposition of these concepts, see Stephen E. Henderson, *Expectations of Privacy in Social Media*, 31 Miss. C. L. Rev. 227, 229-34 (2012).

124. Westin, Historical Perspectives, *supra* note 115 at 6.

125. *See* Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all."); Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-first Century*, 65 Ind. L.J. 549, 564-66 (1990); Burrows v. Superior Court, 529 P.2d 590, 596 (Cal. 1974) (relying on the necessity of a bank account); People v. Jackson, 452 N.E.2d 85, 89 (Ill. App. Ct. 1983) (same); State v. McAllister, 875 A.2d 866, 874 (N.J. 2005) (same); People v. Chapman, 679 P.2d 62, 67 (Cal. 1984) (relying on the necessity of the telephone); People v. Sporleder, 666 P.2d 135, 141 (Colo. 1983) (same); People v. DeLaire, 610 N.E.2d 1277, 1282 (Ill. App. Ct. 1993) (same); State v. Hunt, 450 A.2d 952, 955-56 (N.J. 1982) (same); State v. Boland, 800 P.2d 1112, 1117 (Wash. 1990) (relying on the necessity of trash collection); State v. Morris, 680 A.2d 90, 95 (Vt. 1996) (same).

Standard 25-3.4 Need for regulation

Legislatures, courts that may act in a supervisory capacity, and administrative agencies should therefore carefully consider regulations on law enforcement access to and use of records maintained by institutional third parties. These standards provide a framework for that consideration.

Commentary to Standard 25-3.4

As noted in the Introduction, the federal government and all fifty states regulate law enforcement access to and use of certain types of third party records.[126] The purpose of these Standards is to assist legislatures, courts, and agencies by providing a framework for making these types of determinations, thereby bringing greater consistency to existing law and where necessary framing new law that accounts for changing technologies and social norms, the needs of law enforcement, and the interests of privacy and social participation.

One context in which some might find these considerations relevant is not within the scope of these Standards—constitutional interpretation. Although aspects of these Standards, including the privacy factors of Standard 25-4.1, are derived from constitutional decisions, it is not the place of Criminal Justice Standards to direct courts in their constitutional interpretation. Thus, while courts might independently find the concepts and articulations of the Standards to be of use in interpreting their respective constitutions, the Standards limit their judicial scope to courts acting in a supervisory capacity, the scope of which authority varies by jurisdiction.

Decision makers should avoid the false dichotomy of "privacy versus security." The two are sometimes misrepresented as if there is a unitary dial: if we turn up privacy, we get less security, and if we turn down privacy, we get more security. Security and privacy are viewed as a zero-sum tradeoff. In the both humorous and telling words of scholar Daniel Solove, this false dichotomy has become so ingrained "that people seem to associate being inconvenienced and being intruded upon with secu-

126. *See, e.g.,* 9 C.J.S. Banks and Banking § 269 (summarizing restrictions on government access to bank records); Tracy A. Bateman, *Search and Seizure of Bank Records Pertaining to Customer as Violation of Customer's Rights Under State Law*, 3 A.L.R.5TH 453 (1995).

rity. So if the government wants to make people feel more secure, all it needs to do is make them feel more uncomfortable and exposed."[127]

Information security expert Bruce Schneier is a frequent critic of such "security theater,"[128] and he corrects this misperception: "Too many people wrongly characterize the debate as 'security versus privacy.' . . . Liberty requires security without intrusion, security plus privacy."[129] In other words, there is no doubt that there is a relation between security and privacy, in that a change to one will sometimes affect the other.[130] But sometimes it is possible to increase security without decreasing privacy, sometimes a decrease to privacy leads to no meaningful increase in security, and sometimes what seems a decrease to privacy is, in greater scope, an increase. While law enforcement infringes privacy with the goal of protecting public safety, businesses infringe privacy for monetary gain, and criminals infringe privacy for a variety of motives including monetary gain. Thus, law enforcement investigates and deters a variety of privacy-infringing crimes, such as the hacking of computers, the theft of sensitive corporate information, and the illegal interception of communications. It is therefore possible for restrictions upon law enforcement to lead to a decrease in citizens' privacy in favor of criminals.

Our goal as a nation has always been not merely to be safe, but to be *secure*, and such security requires both safety and privacy. Thus, perhaps in this context it is most helpful to articulate that *safety* and privacy are related and can affect one another, but that *security* requires an ample measure of both, and decision makers should recognize the full complexity of these relationships.[131]

---

127. Daniel J. Solove, Nothing to Hide: The False Tradeoff between Privacy and Security 35 (Yale University Press 2011).

128. *See* Bruce Schneier, *Beyond Security Theater*, 427 New Internationalist 10 (2009), available at http://www.schneier.com/blog/archives/2009/11/beyond_security.html (last visited June 13, 2012).

129. Bruce Schneier, *The Eternal Value of Privacy*, http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70886 (last visited June 13, 2012).

130. In the words of the Eleventh Circuit, "[T]he Fourth Amendment embodies a value judgment by the Framers that prevents us from gradually trading ever-increasing amounts of freedom and privacy for additional security." Bourgeois v. Peters, 387 F.3d 1303, 1312 (11th Cir. 2004).

131. Thus, the Fourth Amendment exists to ensure "the right of the people to be *secure* in their persons, houses, papers, and effects." U.S. Const. amend. IV (emphasis added).

Part IV. Categorization of Information and Protection

Standard 25-4.1 Categories of information

Types of information maintained by institutional third parties should be classified as *highly private*, *moderately private*, *minimally private*, or *not private*. In making that determination, a legislature, court, or administrative agency should consider present and developing technology and the extent to which:

Commentary to Standard 25-4.1

Before a decision maker can decide what restraints to place upon law enforcement access (Part V), it must determine how private the information is. The extent to which the information is private will typically determine how protected is the information according to Standard 25-4.2(a), and thus determine what restraint should be placed upon law enforcement access under Standard 25-5.3. There may be situations, however, in which the marginal cost to effective law enforcement of being permitted to access that information only upon that restraint is unacceptable. In that case, according to Standard 25-4.2(b), a decision maker can reduce the level of protection. It is very important, however, that these two decisions be kept separate and sequential. If they are conflated, the more amorphous but equally important privacy interests are likely to be unfairly discounted.

Privacy is a divisible commodity, meaning information often retains some degree of privacy despite being shared.[132] Nonetheless, disclosures can affect privacy, and this Standard attempts the difficult work of determining the degree of privacy in information provided to and residing with an institutional third party. On the one hand, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a

132. *See* Commentary to Standard 25-3.3, *supra* p. 49.

subject of . . . protection."[133] But on the other hand, information provided only to an intimate, or to a service provider upon effective guarantee of confidentiality, remains highly private.

Unfortunately, while people typically agree on the extremes—e.g., that medical diagnoses are more private than records of utility consumption—there are few bright lines in privacy, and there will be reasoned disagreements in many cases. The best that can be done, therefore, is to provide four factors that should be considered in making this determination and some examples of their application. As in any multi-factor test, in some instances one factor will predominate and in other instances it will be a different factor. That careful thought is required in the factors' application does not negate their utility.

In determining the privacy classification of a record, what is relevant is the information that would be disclosed should the government request be granted. In other words, if law enforcement were to seek only name and address information from a bank record, the appropriate question is how private is name and address information, not how private are bank records. Thus, this Standard classifies types of information, and Standard 25-4.2 relates a record to the type of information it contains.

When a novel technology is at issue, a decision maker must carefully consider the function and use of that technology. Technology has always driven changes in our privacy laws and theory. For example, it was the newly invented portable camera in 1888 that led Samuel Warren and Louis Brandeis to write their seminal article on privacy,[134] and the Supreme Court has stated as follows with respect to modern electronic communications:

> The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment . . . . The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. . . . Prudence counsels caution before the facts in the instant case are used to establish far-

133. Katz v. United States, 389 U.S. 347, 351 (1967).

134. *See* Lori Andrews, I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy 49 (Free Press 2011).

> reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees . . . . Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior.[135]

(a) the initial transfer of such information to an institutional third party is reasonably necessary to participate meaningfully in society or in commerce, or is socially beneficial, including to freedom of speech and association;

Commentary to Standard 25-4.1(a)

One reason a transfer can be considered privacy lessening, and in the Fourth Amendment context has often been held to eliminate a reasonable expectation of privacy,[136] is the notion of assumption of risk: if one chooses to convey information to a third party, he or she accepts the risk that the information will somehow be obtained from that party, including by law enforcement. Of course, it begs the question to presume that there must therefore be no restraint upon law enforcement access, for it is the law that defines what risk is thereby assumed. Even were there to be no restraint upon voluntary third party-initiated dissemination, it would not follow that there should be no restraint upon law enforcement-initiated access.

Nonetheless, it is logical to consider assumption of risk, in that what is given to even one person or entity is more likely to be further disseminated than before. It is not alone determinative, however, because privacy is not secrecy. Instead, secrecy is merely one form of privacy. Privacy is the more encompassing ability to control what information about oneself is known to others, and for what purposes that information is used.[137] Thus, we often expect privacy despite revealing information, and many existing laws so recognize.[138]

Because privacy is fundamentally about control, information sharing is least likely to be privacy limiting when that sharing is necessary to participate meaningfully in society or in commerce. It is one thing to

135. City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010) (internal citations omitted).
136. *See, e.g.,* United States v. Miller, 425 U.S. 435, 443 (1976).
137. *See* Commentary to Standard 25-3.3, *supra* p. 49.
138. Some of these laws are discussed in the examples that follow.

talk of "assuming" a risk of disclosure—and thus in part voluntarily waiving a degree of privacy—when a transfer is genuinely voluntary, but quite another when it is impossible to participate meaningfully in current society or commerce without making that transfer.

Similarly, if a transfer is conducive to other values, especially constitutionally enshrined ones like the freedoms of speech and association, the law should be most wary of chilling it. In the words of Justice Sotomayor, "Awareness that the government may be watching chills associational and expressive freedoms."[139] And in a recent Fourth Amendment case, the Supreme Court opined that "[c]ell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy."[140]

Lower courts have thus sometimes rejected government attempts to subpoena expressive records from a third party based on the concern that permitting such access would chill such beneficial, and constitutionally protected, transfers going forward.[141] In Colorado, the state constitution requires an adversarial hearing before even a warrant can be used to access expressive third party records:

> Bookstores are places where a citizen can explore ideas, receive information, and discover myriad perspectives on every topic imaginable. When a person buys a book at a bookstore, he engages in activity protected by the First Amendment because he is exercising his right to read and receive ideas and information. Any governmental action that interferes with the willingness of customers to purchase books, or booksellers to sell books, thus implicates First Amendment concerns. Anonymity is often essential to the successful and uninhibited exercise of

139. United States v. Jones, 565 U.S. __, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

140. City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010).

141. *See* Amazon.com v. Lay, 2010 WL 4262266, *10-12 (W.D. Wash. 2010); *In re* Grand Jury Investigation of Possible Violation of 18 U.S.C. Section 1461, 706 F. Supp. 2d 11, 16-23 (D.D.C. 2009); *In re* Grand Jury Subpoena to Amazon.com Dated August 7, 2006, 246 F.R.D. 570, 572-74 (W.D. Wisc. 2007).

> First Amendment rights, precisely because of the chilling effects that can result from disclosure of identity.[142]

Example: Content of Private Communications

Existing ABA Standards relate to communications surveillance,[143] and nothing herein is meant to suggest altering those specific rules. Nonetheless, it is helpful to consider how this specific and familiar type of third party information fits within the framework of these Standards.

Telephone conversations have long furthered the freedoms of expression and association, and now electronic mail and other electronic communications do the same. Moreover, both are necessary to participate meaningfully in society and in commerce. In *Katz v. United States*, the Court recognized "the vital role that the . . . telephone has come to play in private communication,"[144] and several courts have more recently recognized the same in the context of determining state constitutional protections.[145] Although electronic communications are more novel, their adoption has been even more dramatic.[146] Both modes of communica-

142. Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044, 1052 (Colo. 2002) (en banc). Although the First Amendment and its state analog were both implicated, the court ultimately decided the case as a matter of the more protective state constitutional law. *See id.* at 1056.

143. ABA Standards for Criminal Justice, Electronic Surveillance, Section A: Electronic Surveillance of Private Communications (3d ed. 2001).

144. 389 U.S. 347, 352 (1967).

145 *See* People v. Chapman, 679 P.2d 62, 67 (Cal. 1984) ("Doing without a telephone is not a realistic option for most people."); People v. Sporleder, 666 P.2d 135, 141 (Colo. 1983) ("A telephone is a necessary component of modern life. It is a personal and business necessity indispensable to one's ability to effectively communicate in today's complex society."); State v. Hunt, 450 A.2d 952, 955-56 (N.J. 1982) ("The telephone has become an essential instrument in carrying on our personal affairs.").

146. According to the Pew Internet & American Life Project, 80% of American adults use the Internet. *Trend Data (Adults)*, http://www.pewinternet.org/Static-Pages/Trend-Data-%28Adults%29/Whos-Online.aspx (last visited June 14, 2012). Of those internet users, 91% use electronic mail. *Trend Data (Adults)*, http://www.pewinternet.org/Trend-Data-%28Adults%29/Online-Activites-Total.aspx (last visited June 14, 2012). Eighty two percent get online daily, and 59% send email daily. *Trend Data (Adults)*, http://www.pewinternet.org/Trend-Data-%28Adults%29/Online-Activities-Daily.aspx (last visited June 14, 2012).

When the Supreme Court decided *Katz* in 1967, approximately 88% of households had a telephone, but that was almost 100 years after the first deployments of that device. *See* Webb & Associates, *Telecommunications History Timeline*, http://www.webbcon-

tion require transferring the content to the communications provider. Since that required transfer is necessary to participate meaningfully in society and in commerce and is socially beneficial, the first factor weighs in favor of considering the content of communications more private.

Example: Information Relating to Communications

Telephonic and electronic service providers retain both customer account information (e.g., physical contact information, telephone number, and email address) and records concerning the communications in which customers engage (e.g., the telephone numbers and email addresses of those with whom one communicates). The former ("subscriber information") is no different than the information retained by a large variety of merchants, but the latter is more unique and is considered here. For this factor, the analysis is identical to that for the content of communications: the transfer is necessary to participate in the service, the service is necessary to participate meaningfully in society and in commerce, and the service is socially beneficial. Thus, this factor weighs in favor of considering information relating to communications to be more private.

Example: Medical Diagnoses, Treatments, and Prescriptions; Utility Consumption

While medical records and utility consumption might ordinarily be strange bedfellows, they present the apex of this first factor in that both can be necessary to sustain life, and the transfer of information is necessary to obtain the services.[147] Therefore, this first factor weighs in favor of considering this information more private. Considering them together not only serves the purposes of brevity, but has the added advantage of demonstrating that each factor is just that: only one factor. Ultimately, a decision maker is likely to impose very different regulations for these two categories.

---

sult.com/hist-time.html (follow "The Late 1800s" hyperlink) (last visited June 14, 2012); U.S. Census Bureau, *Statistical Abstract of the United States* 497 (1969), *available at* http://www2.census.gov/prod2/statcomp/documents/1969-07.pdf (last visited June 14, 2012).

147. Obviously not all of our utility consumption is vital, but at least to the sick, the young, and the elderly it is essential to have heating in the winter and/or cooling in the summer, and for all of us water is necessary to sustain life.

Example: Financial Account and Transaction Records

"Financial account records" is used to mean account information not particular to any transaction. Hence, account records would include customer contact information, balance, credit limit, billing cycle and similar terms of the account. "Financial transaction records" is used to mean information particular to a transaction, including credit card transactions, debit card transactions, and bank account transactions (e.g., a purchase at Amazon.com or Macy's for $73.32). Because application of the privacy factors is mostly identical, the two categories are considered together.

It seems self evident that in the twenty-first century one cannot participate meaningfully in commerce without making bank and credit/debit card transactions. We rely on credit or debit cards for everything from e-commerce to proving identity (e.g., using any major credit card to check in at an airline), and to making as routine a purchase as gasoline. Although writing checks is therefore becoming less common, we use internet banking to pay our bills.[148] As long ago as 1974, the California Supreme Court recognized that "it is impossible to participate in the economic life of contemporary society without maintaining a bank account."[149] The necessity of having these accounts and therefore of creating these records cannot seriously be questioned. Thus, the first factor weighs in favor of considering this information more private.

148. According to the Pew Internet & American Life Project, 61% of internet users engage in online banking. *Trend Data (Adults)*, http://www.pewinternet.org/Trend-Data-%28Adults%29/Online-Activites-Total.aspx (last visited June 14, 2012).

149. Burrows v. Superior Court, 529 P.2d 590, 596 (Cal. 1974). *Accord* People v. Jackson, 452 N.E.2d 85, 89 (Ill. App. Ct. 1983) ("Since it is virtually impossible to participate in the economic life of contemporary society without maintaining an account with a bank, opening a bank account is not entirely volitional and should not be seen as conduct which constitutes a waiver of an expectation of privacy.") (citing *Burrows*); State v. McAllister, 875 A.2d 866, 874 (N.J. 2005) ("[I]n contemporary society, it is the rare citizen who 'socks away' cash in the proverbial mattress. Instead, citizens customarily deposit money in bank accounts, which have become an indispensable part of modern commerce. As a consequence, numerous participants in our nation's economic life leave behind detailed financial dossiers.").

Example: Internet Protocol Address; Full Uniform Resource Locator of World Wide Web Browsing

Just as no two entities can have the same postal address, every end system on the Internet must have a unique Internet Protocol ("IP") address, which looks something like 157.166.226.26 in version four of the protocol.[150] That particular number belongs to news organization CNN, and thus one could enter http://157.166.226.26 in a World Wide Web browser (e.g., Firefox) to visit the front page of CNN's website. Of course, a business can internally further route postal mail, and CNN can do the same for internet traffic. But IP Address 157.166.226.26 uniquely belongs to CNN.[151] Because strings of numbers are not convenient for people to recall, we typically use hostnames in their place. In the case of CNN, www.cnn.com equates to 157.166.226.26. In the case of search engine Google, www.google.com equates to 209.85.227.103.[152] An IP address thus identifies the entity with which one is communicating, and also uniquely identifies the communicating party.[153] It must be communicated to third parties in order to use the Internet.[154]

A Uniform Resource Locator ("URL") is the unique address to content on the World Wide Web.[155] It might tell no more information than the IP address, in that the URL http://www.cnn.com directs a browser to download the front page to the website for CNN. If one searches for "celebrity" within CNN News, however, then the URL is something like this: http://www.cnn.com/search/?query=celebrity. Similarly, the URL http://www.google.com means only that someone visited Google's search engine. But if that person searches for ambidextrous girls with red hair, the URL will include something like http://www.google.com /search?=ambidextrous+girls+with+red+hair.[156] If that person searches

150. It would have 16 decimal numbers separated by periods in the more recent version six. *See* http://en.wikipedia.org/wiki/IP_address (last visited June 14, 2012).

151. Because content can be further internally routed, it is possible for a single IP address to host multiple websites.

152. In practice websites often use multiple IP addresses to distribute the user load.

153. *See* State v. Reid, 945 A.2d 26, 28 (N.J. 2008). Most of us use a "dynamic" IP address assigned by, and therefore registered to, our service provider. *See id.* at 28-29.

154. *See id.* at 29, 33.

155. For further information see http://en.wikipedia.org/wiki/Uniform_Resource_Locator (last visited June 14, 2012).

156. The actual URL will contain many further characters, the meaning of some of which is not apparent without further information.

for "breast cancer symptoms men," after searching for "breast cancer symptoms," the URL will be something like http://www.google.com/search?=breast+cancer+symptoms+men&aq=breast+cancer+symptoms. And whereas the IP address for www.webmd.com is 208.93.170.17, the URL for that site's information on breast cancer in men is http://www.webmd.com/breast-cancer/guide/breast-cancer-men.

The vast content available on the Internet and the ability it provides to communicate with disparate persons without regard to geography, further the freedoms of speech and association. Although perhaps internet access is not yet necessary to participate meaningfully in society and commerce in the sense that heating, medical diagnoses, and banking are, it is increasingly becoming so. For many, the Internet is the preeminent vehicle via which they obtain information about the world and express their views thereon, and via which they engage in commerce. According to the Pew Internet & American Life Project, 80% of adult internet users use the Internet to obtain health and medical information, 76% use the Internet to get news, and 61% use it more specifically to follow politics.[157] Seventy-eight percent use the Internet to research purchases, and 71% use it to make purchases.[158] Thus, there is great concern for the "digital divide" between those who have such access and those who do not.[159] In the words of the New Jersey Supreme Court,

> [Internet Service Provider] records share much in common with long distance billing information and bank records. All are integrally connected to essential activities of today's society. Indeed, it is hard to overstate how important computers and the Internet have become to everyday, modern life. Citizens routinely access the Web for all manner of daily activities: to gather information, explore ideas, read, study, shop, and more.[160]

157. *Trend Data (Adults)*, http://pewinternet.org/Trend-Data-%28Adults%29/Online-Activites-Total.aspx (last visited June 14, 2012).

158. *Id*.

159. *See, e.g., Mr. Obama's Internet Agenda*, N.Y. Times, Dec. 16, 2008, at A36. *See also* Chris Nicholson, *Internet Comes Before Electricity*, N.Y. Times, Feb. 2, 2009, at B4 (describing installation of a satellite dish for internet in a remote Kenyan outpost); Pew Internet & American Life Project, *Digital Divide*, http://pewinternet.org/topics/Digital-Divide.aspx (last visited June 14, 2012).

160. State v. Reid, 945 A.2d 26, 33 (N.J. 2008).

This first factor therefore weighs in favor of considering IP addresses and URLs to be more private. As far as necessity, it perhaps does not tilt as strongly as absolutely necessary transfers like medical diagnoses, but given the Internet's First Amendment implications it is nonetheless weighty.

Example: Location; Geographic Vicinity

Precise location or more general geographic vicinity might be transferred to a third party for a number of different purposes. In order to communicate via mobile phone, a service provider must know which transmission tower is nearest the phone even when a call is not in progress.[161] At one time this provided only geographic vicinity, but the number of cell towers is dramatically increasing, and via triangulation of signals between the nearest towers, a cell phone provider can determine and record a very precise location.[162] Location must likewise be provided to a third party recommending nearby businesses or other sites of interest, and in order to provide the convenience of automated toll collection.

Different location-based services will be more or less important to constitutionally protected interests, but with mobile telephony the contribution to the freedoms of expression and association are quite strong. For many years arguably this contribution was tempered by the ready availability of, and heavy reliance upon, traditional landline telephones. But as mobile phone usage increases and the use of landlines correspondingly decreases, particularly among certain demographics, this may have changed.[163] Not only do 88% of American adults own a mobile

161. *See How Cell Phones Work*, http://www.howstuffworks.com/cell-phone.htm (last visited June 14, 2012). Traditional landline telephony has of course always provided precise location, because the service provider knows where the equipment is located (e.g., either a specific pay phone, a line in a specific hotel, or a line in a home). But it only conveys location information when a call is underway, whereas a mobile phone tracks location anytime the phone is active.

162. *See* H.R. Subcomm. on the Const., Civ. Rights, and Civ. Liberties of the Jud. Comm., *ECPA Reform and the Revolution in Location Based Technologies and Services*, 111th Cong. 15, 20, 26-27, 30, 95 (June 24, 2010) (testimony of Professor Matt Blaze).

163. There are over 285 million active wireless subscriber accounts in the United States. In re Application of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 834 (S.D. Tex. 2010). They account for over 2.2 trillion minutes of use and 1.56 trillion text messages. *Id.*

phone,[164] but 46% are users of the more sophisticated smartphones.[165] Protestors use their mobile phones to communicate with interested parties,[166] and concerned citizens use them to record possible police abuse.[167] Thus, in refusing to decide the Fourth Amendment status of pager communications, the Supreme Court noted the following: "Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy."[168]

(b) such information is personal, including the extent to which it is intimate and likely to cause embarrassment or stigma if disclosed, and whether outside of the initial transfer to an institutional third party it is typically disclosed only within one's close social network, if at all;

Commentary to Standard 25-4.1(b)

It is unassailable that some information is more personal than other information, like medical diagnoses compared to contact information (name, address, and telephone number). But apart from such extremes, it is no easy task to determine just how personal given information is, and thus there is an obvious administrative benefit to a legal rule that does not require such differentiation.

Hence, in the Fourth Amendment context of the home, the Supreme Court in *Kyllo v. United States* refused to develop "a jurisprudence specifying which home activities are 'intimate' and which are not."[169]

164. Pew Internet & American Life Project, *Trend Data (Adults)*, http://pewinternet.org/Trend-Data-%28Adults%29/Device-Ownership.aspx (last visited June 14, 2012).

165. Pew Internet & American Life Project, *Nearly Half of American Adults are Smartphone Owners*, http://pewinternet.org/Reports/2012/Smartphone-Update-2012.aspx (last visited June 14, 2012).

166. *See* Russ Buettner, *Judge Orders Twitter to Turn Over Protester's Messages*, N.Y. Times, July 3, 2012; Jennifer Preston, *Protesters Look for Ways to Feed the Web*, N.Y. Times, Nov. 25, 2011.

167. Eunice Lee, *Watching the Watchmen: ACLU Offers Citizens 'Stealth' App to Record Cops*, Star-Ledger, July 3, 2012; ACLU, *The App Place: Police Tape*, http://www.aclu-nj.org/yourrights/the-app-place/.

168. City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010).

169. 533 U.S. 27, 38-39 (2001).

But the Court was able to decline such a jurisprudence only because it could hold that the use of sense-enhancing technology to determine *any* information regarding the interior of the home constitutes a search typically requiring a warrant supported by probable cause.[170] In other words, *all* home activities are intimate so far as the Fourth Amendment is concerned. Because it would unduly cripple law enforcement to apply that same rule to all third-party records, it is impossible to avoid making distinctions based on the personal nature of information.[171]

One manner of grading intimacy is via scientifically constructed public surveys.[172] No matter the difficulty in their implementation and interpretation, such surveys are superior to what has often happened in the constitutional arena, where justices instead simply declare alleged social expectations without foundation.[173] The sense of a legislature is a more defensible reflection of general social norms and understandings than that of an unelected judge, but legislators too should consider social science data or other evidence. In any survey it is critical that the right question be asked, which for this factor is whether the information is considered personal, not the ultimate conclusion of whether law enforcement ought to be able to access that information. Law enforcement can access information no matter how personal (this factor), and indeed no matter how private (the sum of all four factors), so long as there is adequate justification.

Sometimes the reaction to a disclosure will reveal societal attitudes, as when it came to light that employees of Hewlett Packard had obtained the phone records of board members in order to investigate alleged

170. *Id*. at 34.

171. The other bright-line alternative (i.e., requiring little or no justification for access to all third party records), is just as unacceptable to legitimate privacy interests.

172. *See* Christopher Slobogin, Privacy at Risk: The New Government Surveillance and the Fourth Amendment 183-185 (University of Chicago Press 2007) (describing results of such a survey).

173. *See, e.g.,* Smith v. Maryland, 442 U.S. 735, 742-43 (1979) (alleging without support what telephone customers "typically know"); *id.* at 749 n.1 (Marshall, J., dissenting) (chiding the court majority for this assertion); Georgia v. Randolph, 547 U.S. 103, 113 (2006) (alleging without support the norms of home entry when confronted with conflicting cotenants); *id*. at 129-30 (Roberts, J., dissenting) (chiding the court majority for this assertion); State v. Hempele, 576 A.2d 793, 803 (N.J. 1990) (alleging without support how persons typically feel about privacy of trash); Mont. Human Rights Div. v. City of Billings, 649 P.2d 1283, 1287-88 (Mont. 1982) (alleging without support that employees expect privacy in their records).

information leaks.[174] The backlash cost chairwoman Patricia Dunn her job, and resulted in the passage of anti-pretexting legislation at both the state and federal level, a $14.5 million civil settlement, and the filing of both state and federal criminal charges.[175] It is readily apparent that people and their elected representatives consider phone records personal despite their retention by the telecommunications provider.

Sometimes the reaction to law enforcement conduct will reveal the personal nature of information. When the Supreme Court had to determine whether a public school student had a Fourth Amendment reasonable expectation of privacy that was invaded by a strip search, it looked to "the consistent experiences" and "common reaction" of young persons subjected to such searches as gathered by social workers and psychologists.[176]

Sometimes the practices of third parties will provide clues as to what information is more personal. Because there are both security costs and potential inefficiencies in securing information, that some information is secured while other information is not indicates that at least the third party likely believes the former information to be more personal.

To the extent it is unreliable or unrealistic to directly survey how personal given information is, or even to rank information on a scale, and where other evidence is lacking, it might be possible to empirically study what information typically remains within close social networks. According to social network literature, most information that we reveal never extends beyond two degrees of separation, meaning it is revealed to only one other person beyond the initial revelation.[177] As such, it is more personal than information that is routinely known outside one's social network.[178]

---

174. *See* Damon Darlin, Ex-Chairwoman Among 5 Charged in Hewlett Case, N.Y. Times, Oct. 5, 2006, at A1.

175. *Id.*; Jim Hopkins & Jon Swartz, *Investigations Continue at HP*, USA Today, Oct. 5, 2006, at B2; Ellen Nakashima, *HP, Calif. Settle Spying Lawsuit*, Wash. Post, Dec. 8, 2006, at D1; Jordan Robertson, *U.S. Wins First Guilty Plea in HP Boardroom Spy Probe*, Phil. Inquirer, Jan. 13, 2007, at C2; 18 U.S.C. § 1039 (federal anti-pretexting legislation).

176. Safford Unified School District #1 v. Redding, 129 S. Ct. 2633, 2641-42 (2009) (relying on amicus briefs authored by social workers and school psychologists).

177. *See* Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. Chi. L. Rev. 919, 967 (2005).

178. *See id*. at 934.

Some state courts have sought to differentiate how personal information is in determining constitutional restraints upon government access. Thus, the Supreme Court of Pennsylvania refused to restrict government access to name and address information held by a bank, despite that court's policy of generally restricting access to bank records: "A person's name and address do not, by themselves, reveal anything concerning his personal affairs, opinions, habits or associations."[179] Other courts have held that the same is true of power consumption records[180] and driver's license records.[181] Although it is not a records search, a minority of courts have relied upon the personal nature of garbage left for collec-

179. Commonwealth v. Duncan, 817 A.2d 455, 463 (Pa. 2003) (internal quotation marks omitted). *Accord* State v. Chryst, 793 P.2d 538, 542 (Alaska Ct. App. 1990) (refusing to restrict government access to name and address information held by a utility company); State v. Faydo, 846 P.2d 539, 541 (Wash. Ct. App. 1993) (refusing to restrict government access to a name held by a phone company because "[h]is identity is not 'private' in the same sense as is a record of the phone numbers dialed on a subscriber's phone").

180. *See In re* Maxfield, 945 P.2d 196, 207 (Wash. 1997) (Guy, J., dissenting) (Justice Guy wrote for a majority of five justices refusing to restrict access to power consumption information: "A statement that power consumption at a particular address appears to be high discloses no discrete information about an individual's activities, not even the individual's name. . . . The information did not provide any intimate details of the [defendants'] lives or identify their friends or political and business associates. Electrical consumption information, unlike telephone or bank records or garbage, does not reveal discrete information about a customer's activities."); State v. Kluss, 867 P.2d 247, 254 (Idaho Ct. App. 1993); People v. Dunkin, 888 P.2d 305, 308 (Colo. Ct. App. 1994) (adopting reasoning of *Kluss*); Samson v. State, 919 P.2d 171, 173 (Alaska Ct. App. 1996) (same). Although leaving the ultimate issue undecided, the New Jersey Supreme Court recognized this distinction as well. *See* State v. Domicz, 907 A.2d 395, 403 (N.J. 2006).

181. *See* State v. McKinney, 60 P.3d 46, 51 (Wash. 2002) ("[T]he information kept in the drivers' license records does not reveal intimate details of the defendants' lives, their activities, or the identity of their friends or political and business associates. The only information accessed by police from the . . . records were the names and addresses of the registered owners associated with license plate numbers, physical descriptions, and license status.").

tion in granting it constitutional protection,[182] and Illinois courts have done the same for other types of information.[183]

It should be noted that greater *amounts* of information also work a greater intrusion on privacy. For example, an individual bank transaction may tell relatively little about a person, but records over a significant period may form a "virtual current biography" of an individual.[184] Similarly, limited location information may tell very little, but location over a significant period "reveals an intimate picture of the subject's life that he expects no one to have—short perhaps of his spouse."[185] The potential of bank records or location records to provide such a biography makes them more personal,[186] and a legislature or other decision maker might therefore differentiate access regulation according to amount.

Example: Content of Private Communications

The content of telephonic and electronic communications ranges from the most banal to the most personal. For most of us, it is easy to think of examples of the latter because we engage in them routinely, discussing

182. *See* State v. Granville, 142 P.3d 933, 941 (N.M. Ct. App. 2006) ("The contents of a person's garbage are evidence of his most private traits and intimate affairs. A search of one's garbage can reveal eating, reading, and recreational habits; sexual and personal hygiene practices; information about one's health, finances, and professional status; details regarding political preferences and romantic and other personal relationships; and a person's own private thoughts, activities, beliefs, and associations. Almost every human activity ultimately manifests itself in waste products, and any individual may understandably wish to maintain the confidentiality of his refuse.") (internal quotation marks and citation omitted); State v. Tanaka, 701 P.2d 1274, 1276-77 (Haw. 1985); *Hempele*, 576 A.2d at 802-03; State v. Morris, 680 A.2d 90, 94 (Vt. 1996). *See also* People v. Hillman, 834 P.2d 1271, 1281 (Colo. 1992) (Quinn, J., dissenting). The intimate nature of garbage is well demonstrated by an Oregon investigation in which police utilized a garbage pull to obtain a blood-soaked tampon which they tested for drugs, DNA, and seminal fluid. *See* State v. Galloway, 109 P.3d 383, 384 (Or. App. 2005). There are, of course, nonetheless many courts that have refused constitutional protection for garbage. *See generally* Kimberly J. Winbush, *Searches and Seizures: Reasonable Expectation of Privacy in Contents of Garbage or Trash Receptacle*, 62 A.L.R. 5th 1 (1998).

183. *See* People v. Caballes, 851 N.E.2d 26, 48-55 (Ill. 2006).

184. *See* Burrows v. Superior Court, 529 P.2d 590, 596 (Cal. 1974).

185. United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010) (holding unconstitutional prolonged warrantless GPS monitoring of vehicle), aff'd sub nom., United States v. Jones, 132 S. Ct. 945 (2012).

186. *See* People v. Blair, 602 P.2d 738, 745 (Cal. 1979) (holding that, like bank statements, credit card charges provide "a virtual current biography").

topics as varied as our unfiltered feelings about recent events and those with whom we recently interacted, to our feelings for those with whom we are communicating. When personal communications are disclosed they are often the source of public scandal, like the emails between Governor Mark Sanford and his mistress Maria Belen Chapur,[187] the text messages between Mayor Kwame Kilpatrick and his chief of staff Christine Beatty,[188] and the telephone communications of President Bill Clinton and Monica Lewinski.[189]

In a study by professors Christopher Slobogin and Joseph Schumacher, participants considered telephone monitoring to be highly intrusive, akin to the search of a bedroom and second only to a body cavity search.[190] A more recent study by professors Jeremy Blumenthal, Meera Adya, and Jacqueline Mogle replicated this result.[191] Because people so reveal their most intimate information, this factor weighs in favor of considering the contents of private communications more private.

Example: Information Relating to Communications

Communication transaction records are certainly not as personal as the communications themselves, but they alone form a sort of "virtual biography" in that we are in some sense defined by the entirety of the persons with whom we communicate.[192] In a second Slobogin study, participants considered law enforcement access to "phone records"

187. *See* Robbie Brown & Shaila Dewan, *Ending Mystery, A Governor Says He Had an Affair*, N.Y. Times, June 25, 2009 at A1.

188. *See* Susan Saulny & Nick Bunkley, *Detroit's Mayor Will Leave Office and Go to Jail*, N.Y. Times, Sept. 5, 2008, at A13.

189. *See* Todd S. Purdum, *Testing of a President: The Profile; Starr's Report Paints A Many-Sided Portrait*, N.Y. Times, Sept. 14, 1998, at A23.

190. Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look At "Understandings Recognized and Permitted by Society"*, 42 Duke L.J. 727, 738-39 (1993). Although the participants were asked about real-time surveillance rather than records surveillance ("monitoring phone for 30 days"), the personal nature of the communications are the same whether recorded by law enforcement in real time or recorded by a service provider and then later accessed by the government.

191. Jeremy A. Blumenthal et al, *The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy"*, 11 U. Pa. J. Const. L. 331, 358 (2009).

192. *See* People v. DeLaire, 610 N.E.2d 1277, 1282 (Ill. App. Ct. 1993) ("[T]he [dialing] records revealed personal associations and dealings which create a 'biography' which should not be subject to an unreasonable search or seizure.").

and "e-mail addresses sent to and received from" roughly as intrusive as a pat down, a search of a vehicle, and searches of credit card and pharmacy records.[193] Future studies can build upon this one by increasing the sample size, thereby hopefully decreasing the confidence intervals for the intrusiveness rankings and thus permitting more nuanced conclusions.[194]

Example: Medical Diagnoses, Treatments, and Prescriptions; Utility Consumption

Whereas medical records and utility consumption converge for the first privacy factor,[195] they strongly deviate here. Although it is not the case that utility consumption reveals nothing about our activities[196]—after all, if it were, it would be of no interest to the police—it is far less personal than the intimate information we convey to our doctor and pharmacist. Indeed, depending upon the conditions at issue, there is arguably no more personal information than our medical conditions. Thus, in Slobogin's second study participants considered law enforcement access to electricity records to be relatively nonintrusive, similar to a brief traffic stop, but they considered access to pharmacy records to be highly intrusive, similar to a bedroom search.[197] Courts too have recognized that "a person's prescription drug records . . . contain intimate facts of a personal nature,"[198] whereas "[a] statement that power consumption at a particular address appears to be high discloses no

193. Christopher Slobogin, Privacy at Risk: The New Government Surveillance and the Fourth Amendment 184 (University of Chicago Press 2007).

194. For example, although the mean intrusiveness ranking of accessing phone records was 74.1 (on a scale of one to one hundred) and that for accessing pharmacy records was 78.0, the 95% confidence interval is eight for each. *See id.*

195. *See* Commentary to Standard 25-4.1(a), *supra*.

196. *See* Jack I. Lerner & Deirdre K. Mulligan, *Taking the "Long View" on the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 Stan. Tech. L. Rev. 3, 41 ("Electricity consumption patterns generated from advanced metering infrastructure will reveal variations in power consumption that can be associated with various household activities; detailed power consumption information can reveal personal sleep, work, and travel habits, and likely identify the use of medical equipment and other specialized devices (if not ordinary appliances).").

197. Slobogin, Privacy at Risk, *supra* note 193 at 184.

198. Douglas v. Dobbs, 419 F.3d 1097, 1102 (10th Cir. 2005). *See also* State v. Skinner, 10 So.3d 1212 (La. 2009) (citing Dobbs and listing similar cases).

discrete information about an individual's activities[, nor provides] any intimate details of the [customers'] lives."[199]

Example: Financial Account and Transaction Records

Financial transaction records are quite personal.[200] They do not alone indicate precisely what was purchased, but in the aggregate they provide a virtual current biography of our lives.[201] Every time a credit card is swiped, the provider knows where the customer is located and quite a lot about what he or she is doing. The provider will not know that the good purchased was Mein Kampf, but it will know that at 10:42 a.m. this person purchased $13.49 of goods at the Borders book store in Exton, PA, and that fifteen minutes earlier he spent $7.36 at Starbucks down the street. How much we spend, where we spend it, when we spend it, and on what are paradigm examples of intimate information that we typically disclose only in pieces. Other than a spouse or person of equivalent intimacy, there is likely to be no one person that knows as much about our purchasing habits and daily lives as can be discerned from our financial transaction records. Thus, participants in Slobogin's

199. *In re* Maxfield, 945 P.2d 196, 207 (Wash. 1997) (Guy, J., dissenting, but writing for a majority of five justices refusing to constitutionally restrict access to power consumption information). *Accord* State v. Kluss, 867 P.2d 247, 254 (Idaho Ct. App. 1993); People v. Dunkin, 888 P.2d 305, 308 (Colo. Ct. App. 1994); Samson v. State, 919 P.2d 171, 173 (Alaska Ct. App. 1996).

200. For an explanation of the distinction between financial account and transaction records, see Commentary to Standard 25-4.1(a), *supra*.

201. *See* Burrows v. Superior Court, 529 P.2d 590, 596 (Cal. 1974) ("[T]he totality of bank records provides a virtual current biography."); People v. Blair, 602 P.2d 738, 745 (Cal. 1979) (noting that credit card statements can similarly provide a "virtual current biography"); People v. Jackson, 452 N.E.2d 85, 89 (Ill. Ct. App. 1983) ("We believe that it is reasonable for our citizens to expect that their bank records will be protected from disclosure because in the course of bank dealings, a depositor reveals many aspects of her personal affairs, opinion, habit and associations which provide a current biography of her activities."); State v. McAllister, 875 A.2d 866, 874 (N.J. 2005) ("[B]ank records are simply a collection of numbers, symbols, dates, and tables. They are a veritable chronicle of the mundane . . . . However, when compiled and indexed, individually trivial transactions take on a far greater significance. . . . 'Indeed, the totality of bank records provides a virtual current biography.'") (quoting *Burrows*, 529 P.2d at 596); State v. Domicz, 907 A.2d 395, 403 (N.J. 2006) (distinguishing bank records from utility records on this basis).

second study ranked law enforcement access to credit card and bank records as highly intrusive, akin to the search of a car or bedroom.[202]

Reasonable persons may disagree, however, as to whether financial *account* records are more or less personal than financial *transaction* records. On the one hand, even when compiled, financial account records do not create a virtual current biography as do transaction records. They might also be more often exposed to others, given that we reveal the existence of our accounts when we use them in the ordinary course of business and when providing balance and credit limit information when we wish to open a new account or otherwise prove our creditworthiness. However, we have significant control over when we wish to reveal that account information. And for those who consider their purchases "ordinary" but have very meager or very substantial assets, they might far prefer that others know their transaction records than their account records. Therefore, in the aggregate they are perhaps equally personal.

Example: Internet Protocol Address; Full Uniform Resource Locator of World Wide Web Browsing

IP addresses tend to be much less personal than URLs.[203] First, unless using an obfuscating service like Anonymizer.com[204] or Tor,[205] one must reveal his or her computer's IP address to every entity with which he or she communicates online, including every website visited.[206] However, that address is often not publicly associated with our name or other identity, so alone it reveals little.[207]

202. Slobogin, Privacy at Risk, *supra* note 193 at 184. In Slobogin's first study, participants likewise found access to bank records intrusive, but less so than 30 days of telephone monitoring. Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look At "Understandings Recognized and Permitted by Society"*, 42 Duke L.J. 727, 738-39 (1993). This ordering was reversed in the Blumenthal et al. study. Jeremy A. Blumenthal et al, *The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy"*, 11 U. Pa. J. Const. L. 331, 358-59 (2009).

203. For an explanation of IP addresses and URLs, see Commentary to Standard 25-4.1(a), *supra*.

204. *See* www.anonymizer.com (last visited June 14, 2012).

205. *See* https://www.torproject.org (last visited June 14, 2012).

206. *See* State v. Reid, 945 A.2d 26, 29 (N.J. 2008).

207. *See id*.

As to the IP addresses of the computers with which we communicate, one could be looking for most anything on IP address 72.21.210.250, which belongs to Amazon.com. Some IP addresses are more revealing than those for diverse stores like Amazon.com, such as 216.163.137.68 (Playboy), 64.203.109.110 (Republican National Committee), and 72.5.249.143 (Frederick's of Hollywood).[208] Nevertheless, IP addresses are not as revealing as URLs. If one is considering Barry Manilow's *Ultimate Manilow* compact disc, the URL will be something like http://www.amazon.com/Ultimate-Manilow-Barry. Thus, a log of URLs is highly personal because it reconstructs every webpage we visit, whether it concerns a recent sporting contest, political opinion, or a rare medical condition.

For avid users, URLs will form a more complete biography than financial transaction records. Not only can many purchases be made online, but URLs will reveal not only that a purchase was ultimately made, but also potentially what was purchased, and even what one considered purchasing. Thus, URLs are even more personal than bookstore or library records, because URLs log not only everything we ultimately decide worthy of reading, but much that we merely consider reading.

Anecdotally, people consider URLs to be personal. AOL was roundly criticized for its 2006 release of user search queries,[209] and more recently there has been concern with so-called "deep packet inspection," in which computers track what customers do online in order to provide more "relevant" advertising.[210] Participants in Slobogin's second survey considered law enforcement access to websites visited to be highly intrusive, akin to a pat down, a search of a car, and searches of credit card and pharmacy records.[211]

208. *See* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (recognizing that some IP addresses, like some phone numbers, reveal more content than others, but nonetheless considering them all to be non-content information for purposes of legal protection).

209. *See* Tom Zeller Jr., *AOL Acts On Release Of Data*, N.Y. Times, Aug. 22, 2006, at C1.

210. *See* Stephanie Clifford, *Web Privacy On the Radar In Congress*, N.Y. Times, Aug. 11, 2008 at C1.

211. Christopher Slobogin, Privacy at Risk: The New Government Surveillance and the Fourth Amendment 184 (University of Chicago Press 2007).

Example: Location; Geographic Vicinity

Many records reveal an individual's location at one specific time, such as a store receipt. While depending upon the nature of that location the information can be quite personal, the personal nature of location information increases dramatically with technologies like mobile telephony that track, and thus provide to a third party, location over time.[212] Indeed, there is little that seems more personal than a complete record of one's precise movements, whether acquired via direct surveillance or via historic records. In the words of the New York Court of Appeals,

> [t]he whole of a person's progress through the world, into both public and private spatial spheres, can be charted and recorded over lengthy periods . . . . Disclosed in the 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. What the technology yields and records with breathtaking quality and quantity is 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.[213]

Existing empirical data provide some support for these claims, though more work is necessary. In Slobogin's first study, participants considered an officer following a pedestrian in a police car to be relatively nonintrusive, akin to a roadblock stop.[214] But those same participants considered using a beeper to track an automobile to be more intrusive,

---

212. *See* Anne Barnard, *Growing Presence in the Courtroom: Cellphone Data as Witness*, N.Y. Times, July 6, 2009, at A16; John Markoff, *The Cellphone, Navigating Our Lives*, N.Y. Times, Feb. 17, 2009, at D1.

213. People v. Weaver, 12 N.Y.3d 433, 441-42 (2009).

214. Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look At "Understandings Recognized and Permitted by Society"*, 42 Duke L.J. 727, 738 (1993). In a more recent study using the same scenario, that surveillance was considered somewhat more intrusive. *See* Jeremy A. Blumenthal et al, *The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy"*, 11 U. Pa. J. Const. L. 331, 357 (2009).

akin to a pat down.[215] Although both were considered less invasive than a search of bank records,[216] using a beeper to track an automobile tends to reveal information only over short periods, unlike more sophisticated GPS tracking or the accessing of comprehensive location records.[217] Thus, when a unanimous United States Supreme Court held that law enforcement installation and long-term GPS tracking of a vehicle constitutes a Fourth Amendment search, some of the Justices relied upon the personal nature of this information.[218]

Until recently, location over a significant period was practically obscure, because it is costly to physically shadow another person.[219] But now that technology has made location information cheaply available, it is being routinely accessed[220] and is the subject of active debate.[221]

---

215. Slobogin and Schumacher, *supra* note 214 at 738. It was similarly considered more invasive in the more recent study. *See* Blumenthal et al., *supra* note 214 at 357.

216. Slobogin and Schumacher, *supra* note 214 at 738-39. Again, this was replicated in the more recent study. *See* Blumenthal et al., *supra* note 214 at 359.

217. At least this would have been the case at the time of the 1993 study.

218. *See* United States v. Jones, 132 S. Ct. 945, 955-56 (2012) (Sotomayor, J., concurring); *id.* at 957-64 (Alito, J., concurring in the judgment).

219. "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. Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap." *Id.* at 963-64 (Alito, J., concurring in the judgment). "[T]he 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." United States v. Maynard, 615 F.3d 544, 558 (D.C. Cir. 2010), aff'd sub nom., United States v. Jones, 132 S. Ct. 945 (2012). See also *id.* at 565-66 (distinguishing visual from technological surveillance).

220. *See* Bob Sullivan, *What Local Cops Learn, and Carriers Earn, from Cellphone Records*, MSNBC.com, April 18, 2012, http://redtape.msnbc.msn.com/_news/2012/04/18/11252640-exclusive-what-local-cops-learn-and-carriers-earn-from-cellphone-records (last visited June 14, 2012); Eric Lichtblau, *Police Are Using Phone Tracking as a Routine Tool*, N.Y. Times, March 31, 2012.

221. *See, e.g.*, United States v. Graham, 846 F.Supp.2d 384 (D. Md. 2012) (holding cell phone customers lack any reasonable expectation of privacy in historic cell site location records); In re Application of United States for an Order Pursuant to 18 U.S.C. 2703(d), 2012 WL 3260215 (S.D. Tex. 2012) (disagreeing); Anne Barnard, *Growing Presence in the Courtroom: Cellphone Data as Witness*, N.Y. Times, July 6, 2009, at A16; John Markoff, *The Cellphone, Navigating Our Lives*, N.Y. Times, Feb. 17, 2009, at D1; Joelle Farrell, *Plenty of*

Therefore, decision makers will likely have increased information in the near future regarding how personal is location. Technologies are also making it increasingly practical for a person to voluntarily share his or her location, so we will learn whether people limit that sharing to their close social network or share more indiscriminately.[222]

(c) such information is accessible to and accessed by non-government persons outside the institutional third party; and

Commentary to Standard 25-4.1(c)

This factor will very often be neutral: what is more personal according to Standard 25-4.1(b) is less likely to be accessed by private (meaning non-government) persons outside the institutional third party, and what is less personal is more likely to be so accessed. In such cases, it is not meant to further tip the scales. One of the reasons we consider information personal is because we know it is not routinely accessed, and where it is routinely accessed, it is typically not considered personal.

However, there may be instances in which information is personal—it is intimate and social norms are such that the information is not typically disclosed outside one's close social network—but that information is nonetheless not only accessible to, but is routinely accessed by, persons having no authorization from the person to whom the information relates. So long as that access is lawful (Standard 25-4.1(d)),[223] this factor weighs in favor of considering the information less private, so that law enforcement need not alone "shield its eyes."[224]

Cameras Monitor 55,000 Lancaster Residents, Phil. Inquirer, July 6, 2009, at A1 (cameras combined with facial recognition technology can create records of location, and camera surveillance in general raises the question of how personal is location); Bob Drogin, *Keeping a Close Eye on Itself*, L.A. Times, June 21, 2009, at 1.

222. Location might be shared indirectly via the substance of regular Web updates like those sent via the service at twitter.com (see Noam Cohen, *Twitter on the Barricades in Iran: Six Lessons Learned*, N.Y. Times, June 21, 2009 at 4) or can be shared directly via services like Google's Latitude (see www.google.com/latitude (last visited June 14, 2012)).

223. *Cf.* Oliver v. United States, 466 U.S. 170, 183-84 (1984) (ignoring the law of criminal trespass in allowing unrestricted police entry to so-called "open fields"). That private persons tend to be lawbreakers provides no justification for allowing law enforcement to be the same.

224. This is similar to the Fourth Amendment plain view doctrine, via which law enforcement is entitled to make observations from a location at which they are lawfully present. *See* California v. Ciraolo, 476 U.S. 207, 213 (1986) ("The Fourth Amendment pro-

As an example, consider salary. For many of us, this is information that we reveal to few others, and we would be uncomfortable with its public disclosure. Yet for those who work for public institutions and corporations, salary is often publicly available and accessed by curious individuals. This factor permits law enforcement to access that information just as private persons do. What is relevant, however, is not merely that private persons theoretically could access information, but that they in fact do so. If social norms and practical realities are such that others do not access the information—perhaps it is available only onsite at a remote location—then law enforcement is at no disadvantage in needing justification for access. Of course, law enforcement cannot be expected to know what private persons in fact do. But it is legislatures, courts, and administrative agencies that should gathering such relevant information in considering these privacy factors in order to promulgate clear rules that law enforcement can follow.

Although it is not a records search, this factor has been discussed by some courts in the context of garbage pulls, and their analysis is illuminating. In *California v. Greenwood*, the Supreme Court expressed that "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."[225] This is largely correct, except that it is not sufficient that members of the public *could* observe this type of information. Instead, it is necessary that members of the public do observe such information. When private persons could, but do not, access given information, such practical obscurity renders it effectively private. Thus, in the later case of *Bond v. United States*, the Court held that probing a carry-on bag in an "exploratory manner" is restricted by the Fourth Amendment.[226] Although private persons could so probe others' bags, they in fact typically do not.[227] Similarly, in considering the constitutionality of GPS tracking of vehicles, the District of Columbia Circuit noted that "[i]n

---

tection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares."). *See also* Kyllo v. United States, 533 U.S. 27, 40 (2001) (recognizing that Fourth Amendment limits depend on technology not being in "general public use").

225. 486 U.S. 35, 41 (1988). The Court concluded that "society would not accept as reasonable respondents' claim to an expectation of privacy in trash left for collection in an area accessible to the public." *Id*.

226. 529 U.S. 334, 338-39 (2000).

227. *See id*.

considering whether something is 'exposed' to the public . . . we ask not what another person can physically and may lawfully do but rather what a reasonable person expects another might actually do."[228]

On the other hand is the Colorado Supreme Court opinion in *People v. Hillman*.[229] Although the court had previously diverged from federal constitutional doctrine with respect to electronic tracking,[230] telephone records,[231] and bank records,[232] a divided court decided not to restrict police access to garbage.[233] Critical to its reasoning was the "'common knowledge' that members of the public often sort through other people's garbage."[234] So long as this assertion is empirically correct, and those private searches obtained that information sought by the government,[235] it is a correct application of this factor: information is less private if it is routinely accessed by unrelated non-government persons.[236]

Returning to the records context, courts deciding whether to restrain law enforcement access to utility records have therefore looked to whether those records are publicly accessible. Thus in Colorado it was relevant that such records are routinely accessible and apparently

228. United States v. Maynard, 615 F.3d 544, 559 (D.C. Cir. 2010), aff'd sub nom., United States v. Jones, 132 S. Ct. 945 (2012).

229. 834 P.2d 1271 (Colo. 1992).

230. *See* People v. Oates, 698 P.2d 811, 815-16 (Colo. 1985).

231. *See* People v. Timmons, 690 P.2d 213, 216 (Colo. 1984); People v. Corr, 682 P.2d 20, 26-27 (Colo. 1984); People v. Sporleder, 666 P.2d 135, 144 (Colo. 1983).

232. *See* People v. Lamb, 732 P.2d 1216, 1219 (Colo. 1987); Benson v. People, 703 P.2d 1274, 1278 (Colo. 1985); Charnes v. DiGiacomo, 612 P.2d 1117, 1120 (Colo. 1980).

233. *Hillman*, 834 P.2d at 1271.

234. *Id.* at 1275. *See also* State v. 1993 Chevrolet Pickup, 116 P.3d 800, 804 (Mont. 2005) ("While garbage bags oftentimes remain intact until their contents are collected by a designated hauler, it is also common to see homeless people, stray pets and wildlife, curious children, and scavengers rummaging through trash set out for collection.").

235. *See* State v. Hempele, 576 A.2d 793, 805 (N.J. 1990) ("Although a person may realize that an unwelcome scavenger might sort through his or her garbage, such expectations would not necessarily include a detailed, systematized inspection of the garbage by law enforcement personnel.") (internal quotation marks omitted). For example, even in an area in which non-government persons do look through garbage awaiting collection, they are unlikely to test a blood-soaked tampon for drugs, DNA, and seminal fluid. *See* State v. Galloway, 109 P.3d 383, 384 (Or. App. 2005) (police garbage pull doing just that).

236. In the words of the Connecticut Supreme Court, "[a] person's reasonable expectations as to a particular object cannot be compartmentalized so as to restrain the police from acting as others in society are permitted or suffered to act." State v. DeFusco, 620 A.2d 746, 752 (Conn. 1993).

accessed,[237] whereas in New Jersey it was relevant that there was no support for the State's similar assertion.[238] And in granting state constitutional protection to assigned IP addresses, the New Jersey Supreme Court noted that its holding might change if those addresses became routinely available to private persons.[239]

Because this factor is so dependent upon the norms and actions within a particular jurisdiction, this Commentary will not include an application to specific content types. It should once again be stressed that given the second privacy factor (personal nature of the information, Standard 25-4.1(b)), this third factor will often be neutral.

Finally, it is not generally productive to consider the policies of a third party with regard to *internal* dissemination. Law enforcement is of course an outsider with respect to the third party, and therefore this factor considers only access by outsiders. However, where a third party is the bailee of, or conduit for, information intended for others, such as a phone company or internet service provider as to communications content, that total lack of internal dissemination might indicate a higher degree of privacy.

(d) existing law, including the law of privilege, restricts or allows access to and dissemination of such information or of comparable information.

Commentary to Standard 25-4.1(d)

The raison d'etre of these Standards is that decision makers should judiciously reconsider existing rules under the framework herein, if nothing else to ensure consistency in those rules and to account for changing technologies and social norms. Nonetheless, it would be foolhardy to do so without regard to what has come before. Thus, where a decision maker considering law enforcement access to records is not writing on a clean slate, that history should receive careful consider-

237. *See* People v. Dunkin, 888 P.2d 305, 308 (Colo. App. 1994) (finding records available to the public and accessed by real estate professionals and prospective home purchasers).

238. *See* State v. Domicz, 873 A.2d 630, 650 (N.J. Super. Ct. App. Div. 2005) (rejecting State's "unsupported suggestion" that records were available to the public), *rev'd on other grounds*, 907 A.2d 395 (N.J. 2006).

239. *See* State v. Reid, 945 A.2d 26, 35 (2008).

ation. While it may be the case that existing restrictions are either too lenient or too demanding, it may also be that they are ideal.

Most persuasive are previous decisions regarding access to the very same type of information and under the same external circumstances, meaning social norms and technologies have not appreciably changed since the decision was made. Least persuasive is the absence of any action, since there are many reasons that legislation is not enacted, judicial decisions are not written, and executive rules are not drafted that are entirely divorced from a substantive decision that the status quo is ideal.

It is not only, nor even primarily, laws restricting law enforcement that are relevant to this factor. If information cannot be legally accessed and/or disseminated, for whatever reason, it is more private. Where information legally must be accessible or disseminated, it is less private. For example, when the Supreme Court considered whether a government employee had a reasonable expectation of privacy in communications via a government-issued pager, it noted the relevance of state open records laws.[240] And when the District of Columbia Circuit considered location information, it noted the relevance of state statutes, including those limiting civilian conduct.[241] There are, however, fundamental differences between law enforcement access and non-government access, including the former's compulsory process and absence of market alternatives.[242] Therefore, decision makers sometimes decide that law enforcement should be the only restricted party.[243]

As of this drafting, there is little uniformity in laws governing records access among the fifty-one jurisdictions in the United States, meaning

240. *See* City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010).

241. *See* United States v. Maynard, 615 F.3d 544, 564 (D.C. Cir. 2010), aff'd sub nom., United States v. Jones, 132 S. Ct. 945 (2012). Other courts have similarly looked to existing statutory and common law in determining whether an individual has a Fourth Amendment reasonable expectation of privacy. *See e.g.*, Warshak v. United States, 490 F.3d 455, 474-75 (2007) (looking to federal statute in requiring a warrant for email), vacated on other grounds by 532 F.3d 521 (6th Cir. 2008); Doe v. Broderick, 225 F.3d 440, 450 (4th Cir. 2000) (looking to federal statute in requiring a warrant for medical records); DeMassa v. Nunez, 770 F.2d 1505, 1506-07 (9th Cir. 1985) (looking to other constitutional provisions, federal and state statutes, case law, and codes of professional responsibilities in requiring a warrant for attorney files); People v. Gutierrez, 222 P.3d 925, 932-36 (Colo. 2009) (looking to federal and state statutes and case law in requiring a warrant for tax preparer records).

242. *See* Commentary to Standard 25-2.1(f)(ii), *supra*.

243. *See, e.g.*, 18 U.S.C. §§ 2702(a)(3), 2702(c)(6) (generally permitting certain voluntary disclosures but forbidding them to the government).

the fifty states and the District of Columbia. Moreover, some jurisdictions will have entire manners of access (e.g., grand jury investigative subpoena) that others do not, and there are thousands of law enforcement agencies,[244] each with its own internal rules and procedures. Therefore, the following examples focus on federal constitutional law, federal statutory law, and state constitutional law, but are not meant to be all-inclusive, and every jurisdiction must account for the entirety of its own existing law in applying this factor.

Example: Content of Private Communications

The Fourth Amendment requires a warrant for law enforcement wiretapping, meaning acquiring the contents of private communications contemporaneously with their transmission.[245] In addition to allowing use of a warrant, the Stored Communications Act ("SCA") allows the use of a subpoena or "specific and articulable facts" court order to compel disclosure of the contents of stored communications in some circumstances, including the contents of communications greater than 180 days old.[246] The Supreme Court has not addressed whether the SCA complies with the Fourth Amendment, but the Sixth Circuit has held that it does not.[247] It is a potential federal felony for private persons to obtain unauthorized access to stored communications,[248] and entities providing service to the public cannot voluntarily disclose content except in limited

244. The Federal Bureau of Investigation's Uniform Crime Reporting Program compiles data from nearly 17,000 law enforcement agencies. *See* Federal Bureau of Investigation, Uniform Crime Reports, http://www.fbi.gov/ucr/ucr.htm (last visited June 14, 2012).

245. Berger v. New York, 388 U.S. 41 (1967).

246. 18 U.S.C. §§ 2703(a), 2703(b).

247. United States v. Warshak, 631 F.3d 266, 283-288 (6th Cir. 2010).

248. 18 U.S.C. § 2701. This protection exists only so long as the communication remains in "electronic storage," a term defined in 18 U.S.C. § 2510(17) and incorporated by 18 U.S.C. § 2711(1). There is disagreement concerning whether communications remain in electronic storage once they have been received by the intended recipient. *See* Department of Justice Computer Crime and Intellectual Property Section, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 123-27 (2009) (considering such received communications as no longer in electronic storage); Theofel v. Farey-Jones, 359 F.3d 1066, 1075-77 (9th Cir. 2004) (disagreeing).

circumstances, most pertinently where that content was inadvertently obtained and appears to pertain to the commission of a crime.[249]

Example: Information Relating to Communications

There is no Fourth Amendment protection for communication transaction records.[250] The New Jersey Supreme Court has recognized state constitutional protection for internet service provider subscriber information,[251] and therefore would likely protect transaction records.

The Telephone Records and Privacy Protection Act of 2006 made it a federal felony for a private person to obtain fraudulent access to such records.[252] Among the Congressional findings are the following:

> (1) telephone records can be of great use to criminals because the information contained in call logs may include a wealth of personal data;
>
> (2) call logs may reveal the names of telephone users' doctors, public and private relationships, business associates, and more; [and]
>
> (3) call logs are typically maintained for the exclusive use of phone companies, their authorized agents, and authorized consumers.[253]

249. 18 U.S.C. § 2702(b).

250. Smith v. Maryland, 442 U.S. 735 (1979) (holding there is no reasonable expectation of privacy in phone transactional information); United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010) (holding there is no reasonable expectation of privacy in e-mail transactional information and in internet protocol addresses of websites visited); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (same); United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010) (holding there is no reasonable expectation of privacy in internet subscriber information); United States v. Perrine, 518 F.3d 1196, 1204-05 (10th Cir. 2008) (same); United States v. Hambrick, 2000 WL 1062039, *3-4 (4th Cir. 2000) (same); United States v. D'Andrea, 497 F. Supp. 117, 120 (D. Mass. 2007) (same), vacated on other grounds, 648 F.3d 1 (1st Cir. 2011); State v. Mello, 162 N.H. 115, 120 (N.H. 2011) (same under state constitution). *Cf.* State v. Reid, 194 N.J. 386, 399 (N.J. 2008) (holding there is a reasonable expectation of privacy in subscriber information under state constitution).

251. State v. Reid, 945 A.2d 26, 28 (N.J. 2008) (permitting access to subscriber information via grand jury subpoena without notice to subscriber).

252. 18 U.S.C. § 1039.

253. Pub. L. No. 109-476, 120 Stat. 3568 (2007).

Although service providers can typically voluntarily disclose information relating to communications, providers to the public may voluntarily provide that information to the government only in limited circumstances, including to prevent death or serious physical injury.[254] The Telecommunications Act of 1996 likewise restricts voluntary disclosure.[255] Law enforcement-initiated disclosure requires a "specific and articulable" facts court order finding relevance.[256]

Example: Medical Diagnoses, Treatments, and Prescriptions; Utility Consumption

Because of the due process right to medical privacy, either the Due Process clause directly or the Fourth Amendment might restrict law enforcement access to medical records despite the third party doctrine.[257] According to the Supreme Court of Louisiana, the Fourth Amendment and the Louisiana constitutional analog require a warrant to obtain medical and pharmaceutical records.[258] Other courts that recognize federal constitutional protection nonetheless would not require a warrant,[259] and many courts have yet to decide the issue. At least one court has held there to be no federal constitutional restraint.[260] Thus, the federal constitutional law governing law enforcement access to medical records remains variable and unsettled. While some state courts have

254. 18 U.S.C. §§ 2702(a)(3), 2702(c).

255. *See* 47 U.S.C. § 222.

256. 18 U.S.C. §§ 2703(c)(1)(B), 2703(d).

257. *See* Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001) (holding unconstitutional a program of urinalysis testing intended to benefit police). "The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent." *Id.* at 78.

258. State v. Skinner, 10 So.3d 1212, 1218 (La. 2009). *See also* Doe v. Broderick, 225 F.3d 440, 450-52 (4th Cir. 2000) (holding warrantless acquisition unconstitutional).

259. *See* Douglas v. Dobbs, 419 F.3d 1097, 1104 (10th Cir. 2005) (Tymkovich, J., concurring) (not deciding the issue but collecting cases).

260. Jarvis v. Wellman, 52 F.3d 125, 126 (6th Cir. 1995). *See also* People v. Perlos, 462 N.W.2d 310, 318 (Mich. 1990) (holding there is no reasonable expectation of privacy in blood alcohol test results); Williams v. Commonwealth, 213 S.W.3d 671, 681-84 (Ky. 2006) (holding there is no reasonable expectation of privacy in pharmacy records).

held there to be state constitutional protection,[261] that law too remains largely unsettled.

State statutory protections of the physician-patient privilege will provide varying restrictions on medical records access and dissemination.[262] The federal Health Insurance Portability and Accountability Act (HIPAA) restricts disclosure, but rules promulgated pursuant to that Act allow disclosure for law enforcement purposes pursuant to, inter alia, an administrative, trial, or grand jury subpoena.[263] Upon the request of a law enforcement officer, HIPAA also permits disclosure of limited information intended for the identification and location of a suspect or material witness, namely name and address, birth date, social security number, blood type, basic physical description, type of injury, and the date and time of treatment.[264]

As for utility consumption records, the third party doctrine dictates that there is no federal Fourth Amendment protection. Although in several states defendants have sought to restrict government access as a matter of state constitutional law, they have not met with any success.[265]

Example: Financial Account and Transaction Records

A variety of state laws restrict access to and dissemination of bank records,[266] including, in a number of states, constitutional restrictions

261. *E.g.*, King v. State, 577 S.E.2d 764, 765, 767 (Ga. 2003) (holding state constitution permits access either via subpoena with advance notice or search warrant); State v. Bilant, 36 P.3d 883, 887 (Mont. 2001) (requiring probable cause).

262. *See generally* 40A Am. Jur. 2d Hospitals and Asylums § 49 (2008); Wanda Ellen Wakefield, Annotation, *Physician-Patient Privilege as Extending to Patient's Medical or Hospital Records*, 10 A.L.R. 4th 552 (1981).

263. 45 C.F.R. 164.512(f)(1)(ii).

264. 45 C.F.R. 164.512(f)(2).

265. *See* State v. Domicz, 907 A.2d 395, 403-04 (N.J. 2006) (collecting cases).

266. *See generally* Tracy A. Bateman, Annotation, *Search and Seizure of Bank Records Pertaining to Customer as Violation of Customer's Rights under State Law*, 33 A.L.R. 5th 453 (1995). As a statutory example, Oregon law permits law enforcement access either with customer notice or upon a reasonable suspicion court order. *See* Or. Rev. Stat. § 192.565. As a matter of implied contract, consider these words of an Alabama appellate court:

> [W]e note that the records of depositors at banks . . . are not open to general inspection. It is now well settled that absent compulsion by law, a bank may not make any disclosures concerning a depositor's account without the express or implied consent of the depositor. It is implicit in the contract of the bank with its customer or depositor that no information may be disclosed by

upon law enforcement access.[267] Where applicable, the state constitution might require probable cause, a grand jury subpoena, or some other restraint.[268]

At the federal level, there is no Fourth Amendment restraint on law enforcement access.[269] The Right to Financial Privacy Act typically requires a subpoena for government access to bank or credit card records,[270] but permits delaying notice to the customer.[271] The Fair Credit Reporting Act similarly requires a court order or grand jury subpoena to access credit agency records.[272]

As to voluntary dissemination to non-government actors, the Gramm-Leach-Bliley Act declares "the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[273] Financial institutions must develop administrative, technical, and physical safeguards to ensure that confidentiality.[274] The Act's notice requirements[275] are the genesis of the privacy policies bank customers routinely receive.

> the bank or its employees concerning the customer's or depositor's account, and that, unless authorized by law or by the customer or depositor, the bank must be held liable for breach of the implied contract. This principle is reflected in Ala. Code 1975, § 5-5A-43, which sets forth certain limited circumstances under which a bank may disclose financial records of its customers, and in the commentary to that statute, which states that "[c]ustomer records should be disclosed only upon subpoena or court order."

White v. Regions Bank, 729 So.2d 856, 858 (Ala. Civ. App. 1998) (internal citations and quotation marks omitted).

267. *See* Bateman, *supra* note 266 at § 3; Burrows v. Superior Court, 529 P.2d 590, 594-95 (Cal. 1974); People v. Blair, 602 P.2d 738, 745 (Cal. 1979); People v. Mason, 989 P.2d 757, 760-62 (Colo. 1999); Winfield v. Div. of Pari-Mutuel Wagering, 477 So. 2d 544, 548 (Fla. 1985); People v. Jackson, 452 N.E.2d 85, 89 (Ill. App. Ct. 1983); State v. McAllister, 875 A.2d 866, 874 (N.J. 2005); State v. Domicz, 907 A.2d 395, 403 (N.J. 2006) (distinguishing bank records from utility records); Commonwealth v. DeJohn, 403 A.2d 1283, 1291 (Pa. 1979); State v. Thompson, 810 P.2d 415, 418 (Utah 1991).

268. *See, e.g.*, *Mason*, 989 P.2d at 760-62 (permitting either).

269. United States v. Miller, 425 U.S. 435, 443 (1976).

270. 12 U.S.C. § 3407.

271. *Id.* § 3409.

272. 15 U.S.C. § 1681b(a)(1).

273. 15 U.S.C. § 6801(a).

274. *Id.* § 6801(b).

275. *Id.* § 6802.

Example: Internet Protocol Address; Full Uniform Resource Locator of World Wide Web Browsing

Although there is little case law addressing law enforcement access to the Internet Protocol (IP) addresses of websites visited, they are the equivalent of traditional telephony's telephone numbers dialed and of postal mail's addressing information. In each instance, the information must not only be conveyed, but must be used by the provider in order to perform the requested service. Therefore, under the third party doctrine, IP addresses visited receive no Fourth Amendment protection.[276] Some states are nonetheless likely to restrict law enforcement access under their state constitutional analog.[277]

Because a full Uniform Resource Locator (URL) can contain search terms and other information submitted by the user, and alone determines the full content transmitted, it might be considered analogous to the conversations of traditional telephony and the contents of postal mail.[278] If so, it should receive significant Fourth Amendment protection under *Ex parte Jackson*,[279] *Berger v. New York*,[280] and their progeny. But URLs, like IP addresses, are necessarily used by the service provider to provide the requested service. Thus, a court following the third party doctrine could also deem URLs equivalent to unprotected IP addresses and bank records.

A content/non-content distinction is thus nebulous,[281] but it is unfortunately dispositive as to federal statutory protection. The Stored Communications Act broadly defines "contents" as "any information concerning the substance, purport, or meaning of [a] communication,"[282]

---

276. United States v. Forrester, 512 F.3d 500, 509-11 (9th Cir. 2008).

277. *E.g.*, State v. Reid, 945 A.2d 26, 33-34 (2008) (protecting basic customer information held by an internet service provider and indexed by an IP address).

278. *See Forrester*, 512 F.3d at 510 n.6, 511; Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 Wm. & Mary L. Rev. 2105, 2133-43 (2009).

279. 96 U.S. 727 (1877) (postal mail).

280. 388 U.S. 41 (1967) (telephone).

281. *See* Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 Pepp. L. Rev. 975, 1020-23 (2007) (questioning the utility of a content/non-content distinction).

282. 18 U.S.C. § 2510(8). This definition is incorporated into the Stored Communications Act by 18 U.S.C. § 2711(1). The Act defines *wire*, *oral* and *electronic communication*, the latter of which is defined very broadly: "'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in

and generally protects contents by a warrant requirement.[283] Under this broad definition, URLs seem to constitute content,[284] and arguably IP addresses are as well.[285] But the Act so protects contents only as long as they are in "electronic storage" for 180 days or less,[286] and the meaning of "electronic storage" is disputed.[287]

If not deemed content, law enforcement can access such information via a "specific and articulable facts" court order.[288] A customer's own IP address, meaning that assigned to his or her computer, is protected by only a subpoena requirement.[289]

The federal statutory restrictions on service provider-initiated disclosure are addressed above in the context of law enforcement access to the content of private communications[290] and to information relating to communications.[291]

Example: Location; Geographic Vicinity

As of this drafting, the federal constitutional law regarding law enforcement access to location information is in flux, and application of the federal statutory law is equally uncertain as it requires application of several unclear statutes.

In 2012, a unanimous United States Supreme Court held that long-term law enforcement GPS tracking of a vehicle constitutes a Fourth Amendment search.[292] However, the justices employed two differ-

---

whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system . . . ." 18 U.S.C. § 2510.

283. 18 U.S.C. § 2703(a).

284. *See In re* Application of the U.S. for an Order Authorizing the Use of a Pen Register, 396 F. Supp. 2d 45, 49 (D. Mass. 2005).

285. *See* Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 Wm. & Mary L. Rev. 2105, 2167-68 (2009).

286. 18 U.S.C. § 2703(a).

287. *See supra* note 248.

288. 18 U.S.C. §§ 2703(c), 2703(d). In particular, "[a] court order . . . 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." *Id.* § 2703(d).

289. *See* 18 U.S.C. § 2703(c)(2).

290. *See supra* note 249 and accompanying text.

291. *See supra* notes 254-55 and accompanying text.

292. United States v. Jones, 132 S. Ct. 945 (2012).

ent rationales. Justice Scalia, writing for five Justices, relied upon the physical trespass of installing the device, which would not be relevant to non-trespassory records access.[293] One of those five justices, Justice Sotomayor, also wrote separately to address the personal nature of location information and the resulting infringement upon one's reasonable expectation of privacy,[294] and Justice Alito wrote for four Justices who relied solely upon this reasonable expectation of privacy criterion.[295] So, not only are there five justices who find long-term location tracking to infringe upon a reasonable expectation of privacy regardless of physical trespass, but Scalia was careful to note that his trespass rationale is a Fourth Amendment minimum, not its sole protection.[296]

Because the government did not raise the issue below—instead arguing solely that the GPS installation and tracking did not constitute a search—the Court did not decide whether this surveillance requires a warrant.[297] Lower courts are only beginning to grapple with this new precedent, and they were already in disagreement as to whether the Fourth Amendment restricts law enforcement access to historic location information and as to how federal statutory law should be applied.[298]

---

293. *Id.* at 949-53.

294. *Id.* at 955-56 (Sotomayor, J., concurring).

295. *Id.* at 957-64 (Alito, J., concurring in the judgment).

296. "[U]nlike the [Alito] 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." *Id.* at 953.

297. *Id*. at 954.

298. *See* United States v. Graham, 846 F.Supp.2d 384 (D. Md. 2012) (holding there is no reasonable expectation of privacy in historic cell site location information despite *Jones*, and collecting relevant supporting and conflicting case law); *In re* Application of U.S. for an Order Pursuant to 18 U.S.C. 2703(d), 2012 WL 3260215 (S.D. Tex. 2012) (disagreeing). As to prospective access to cell site location information, the Department of Justice tries to combine a certification order under the prospective Pen Trap Statute with a reasonable suspicion order under the retrospective Stored Communications Act, a solution that some courts accept and others do not. *See* Department of Justice Computer Crime and Intellectual Property Section, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 159-61 (2009), available at http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf. As to GPS surveillance of a vehicle see State v. Brereton, __ N.W.2d __, 2013 WI 17, ¶43 (Wis. 2013) (requiring warrant for vehicle location tracking); State v. Zahn, 812 N.W.2d 490, 499 (S.D. 2012) (same); United States v. Ortiz, 878 F. Supp. 2d 515, 536-37 (E.D. Pa. 2012) (same).

The Third Circuit, for example, has held that federal statutes permit a magistrate to choose to require a warrant or to permit a lesser process.[299]

As interpreted by the courts, several state constitutions also require a warrant for law enforcement location tracking,[300] and there are federal restrictions on mobile phone providers choosing to disclose location information.[301]

Standard 25-4.2 Categories of protection

(a) The type of authorization required for obtaining a record should depend upon the privacy of the type of information in that record, such that: records containing *highly private* information should be *highly protected*, records containing *moderately private* information should be *moderately protected*, records containing *minimally private* information should be *minimally protected*, and records containing information *that is not private* should be *unprotected*. If a record contains different types of information, it should be afforded the level of protection appropriate for the most private type it contains.

Commentary to Standard 25-4.2(a)

Once a legislature, court, or administrative agency has used the privacy factors and direction of Standard 25-4.1 to classify a type of information on the privacy hierarchy, it remains to decide what restriction

299. *In re* Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304, 319 (3d Cir. 2010). While district courts agree that law enforcement access to historic cell phone location information requires a court order, some require a warrant supported by probable cause while others permit access upon a demonstration of "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records . . . are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). *See In re* Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 534 F. Supp. 2d 585, 600-01 (W.D. Pa. 2008) (requiring probable cause but also collecting cases to the contrary).

300. *See* People v. Weaver, 12 N.Y.3d 433, 445 (2009); State v. Jackson, 76 P.3d 217, 224 (Wash. 2003); State v. Campbell, 759 P.2d 1040, 1049 (Or. 1988).

301. 47 U.S.C. § 222(f). For relevant legislative history and analysis, see *In re* Application of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 841-43 (S.D. Tex. 2010).

or regulation will be placed upon law enforcement access to records containing that type of information. By design, these Standards do not specify what measure of protection should be given to any particular content type. Instead, they provide a framework via which the appropriate decision maker can make those nuanced judgments that depend upon, among other factors, local social norms, available technologies, and current laws.

The first step in making that judgment is to assign a level of protection solely according to the privacy of the information at issue; thus, records containing *highly private* information should be *highly protected*, records containing *moderately private* information should be *moderately protected*, records containing *minimally private* information should be *minimally protected*, and records containing information *that is not private* should be *unprotected*. If different types of content are commingled in a single record, as will often be the case, then the protection afforded to that record should be dictated by the most private type of information contained therein.[302]

Beginning solely with privacy is fundamentally important, because whereas law enforcement need for a type of information will often rightly be evident and compelling, the effects of inadequately regulating such access can be just as compelling, if often more diffuse and long-term. But because of that more nebulous nature, and because there is often not any party vigorously representing that privacy interest, a decision maker who begins by "balancing" privacy and law enforcement need is prone to unfairly credit the latter, or at least to unfairly discount the former. Thus, the Fourth Amendment, for example, protects the home via a warrant requirement. Absent consent, emergency aid, or probable cause plus exigent circumstances, police cannot enter a home absent a judicial warrant supported by probable cause.[303] It does not matter whether the crime under investigation is a very serious one, whether there is a great deal of that crime occurring, or even that it may be impossible to solve

302. *See* Standard 25-5.5, *infra* p. 109.

303. Payton v. New York, 445 U.S. 573, 603 (1980). *See also* Kirk v. Louisiana, 536 U.S. 635 (2002) (reaffirming the principles and holding of *Payton*); Kyllo v. United States, 533 U.S. 27 (2001) (reaffirming the warrant requirement as applied to sense enhancing technology directed at the home).

that crime absent home entry: the home is very private, and therefore the home is protected by a warrant requirement.[304]

After extensive discussion and debate, however, it was decided that while this is the correct *starting point* for regulating records access, it is not necessarily the correct ending point. Thus, Standard 25-4.2(b) provides an "escape valve" via which a legislature can, in appropriate circumstances, lower the level of protection below this threshold.

(b) If the limitation imposed by subdivision (a) would render law enforcement unable to solve or prevent an unacceptable amount of otherwise solvable or preventable crime, such that the benefits of respecting privacy are outweighed by this social cost, a legislature may consider reducing, to the limited extent necessary to correct this imbalance, the level of protection for that type of information, so long as doing so does not violate the federal or applicable state constitution.

Commentary to Standard 25-4.2(b)

These Standards independently account for law enforcement access where there is emergency need or exigent circumstances.[305] But even absent such exigency, there may be instances in which the marginal cost of applying the threshold of Standard 25-4.2(a) is too great, in that the authorization required by Standard 25-5.3(a) would render law enforcement unable to solve or prevent an unacceptable amount of otherwise solvable or preventable crime, such that the benefits of respecting privacy are outweighed by this social cost. In that case, a legislature—and only a legislature in order to ensure political accountability and adequate

304. "Since we hold to the centuries-old principle of respect for the privacy of the home, it is beyond dispute that the home is entitled to special protection as the center of the private lives of our people. We have, after all, lived our whole national history with an understanding of the ancient adage that a man's house is his castle to the point that the poorest man may in his cottage bid defiance to all the forces of the Crown." Georgia v. Randolph, 547 U.S. 103, 115 (2006) (internal quotation marks and citations omitted). *See also Payton*, 445 U.S. at 596-97 ("The common-law sources display a sensitivity to privacy interests that could not have been lost on the Framers. The zealous and frequent repetition of the adage that a 'man's house is his castle,' made it abundantly clear that both in England and in the Colonies 'the freedom of one's house' was one of the most vital elements of English liberty.").

305. *See* Standard 25-5.4, *infra* p. 108.

information gathering—may consider reducing the level of protection. Of course, any resulting reduction should be the least amount necessary to correct the imbalance (e.g., according records containing highly private information with moderate protection), and a reduction is not possible if it would violate the federal or applicable state constitution. And it is critical that the legislature only consider the marginal cost of the restraint in its calculus. The question is not whether the desired evidence is important to solving or preventing a particular type of crime, nor whether it is important to solve or prevent that type of crime, but only whether the particular restraint would make it difficult to solve that crime. Legislators must take care lest this exception swallow the rule.

For example, hospital admission information, like a medical diagnosis more generally, is likely to be considered highly private according to Standard 25-4.1. If so, according to Standard 25-4.2(a), hospital admission records would be highly protected, and thus according to Standard 25-5.3(a), law enforcement access would typically require a warrant. As demonstrated in the hypothetical park shooting presented in the Introduction,[306] police will routinely require access to certain hospital admission records at the early stages of an investigation. Perhaps a probable cause threshold could be satisfied, in that there is a substantial chance that geographically relevant hospital admission records revealing a wound consistent with a recent crime contain evidence of crime, and de-identified records could reveal whether there were any such admissions.[307] Nonetheless, a legislature might reasonably decide that such a restraint would unacceptably interfere with the timely investigation of serious crime. Perhaps the best evidence for this proposition are the overwhelming number of jurisdictions that require medical providers to affirmatively report such diagnoses even absent a government request.[308] Therefore, a legislature might decide to classify medical

306. *See* Introduction, *supra* p. 11.

307. *See* Standard 25-5.6, *infra* p. 111.

308. *See* Sarah M. Teal, *Domestic Violence: The Quest for Zero Tolerance in the United States and China*, 5 J.L. Society 313, 341 n.166 (2003) (collecting statutes). For other instances of mandatory reporting to law enforcement, see, e.g., Danny R. Veilleux, *Validity, Construction, and Application of State Statute Requiring Doctor or Other Person to Report Child Abuse*, 73 A.L.R.4th 782 (1989); Molly Dickinson Velick, *Mandatory Reporting Statutes: A Necessary Yet Underutilized Response to Elder Abuse*, 3 Elder L.J. 165 (1995); 18 U.S.C. § 2258A (child pornography); L. Richard Fischer, Law of Fin. Privacy ¶ 4.08 (banking suspicious activity reports).

diagnoses relating to gunshot wounds and other violent crime as less protected—perhaps even unprotected—whereas other medical diagnoses would remain highly protected.

Part V. Access to Records

Standard 25-5.1 Consent

Law enforcement should be permitted to access by particularized request any record maintained by an institutional third party if:

(a) the focus of the record has knowingly and voluntarily consented to that specific law enforcement access;

Commentary to Standard 25-5.1(a)

The consent of the person whose privacy is implicated is ample justification for law enforcement records access. The citizen/law enforcement interaction need not be an adversarial one, and in many circumstances a reasonable person would knowingly and voluntary agree to third party records access, either desiring to assist in an investigation or at least to deflect understandable but erroneous suspicion from him- or herself. This Standard is not, however, intended to permit fishing expeditions, and thus it requires a particularized request to which the focus of the record has knowingly and voluntarily acceded. If law enforcement wishes to rely upon something as consent other than knowing and voluntary agreement to this specific access, it should be required to look to Standard 25-5.1(b).

Only knowing and voluntary agreement constitutes consent. The Supreme Court has modified this traditional requirement for purposes of the Fourth Amendment, but for reasons that are rarely applicable to records acquisition. Concerned with whether police could adequately discern knowledge or advise persons of their right to refuse in the unstructured and ever-shifting environment found at the scene of a crime or along a highway, the Court made knowledge a factor in the Fourth Amendment voluntariness inquiry rather than a separate element.[309]

309. Schneckloth v. Bustamonte, 412 U.S. 218, 231-32 (1973). *Cf.* State v. Brown, 156 S.W.3d 722, 731 (Ark. 2004) (requiring knowing agreement for home entry); State v. Ferrier, 960 P.2d 927, 934 (Wash. 1998) (same); Graves v. State, 708 So. 2d 858, 863 (Miss.

Those concerns, however, are greatly reduced, if not eliminated, in the majority of third party records acquisitions, and in those non-exigent instances in which police desire immediate on-the-scene access to third party records, explaining the right to refuse, or otherwise discerning knowledge, should not be an insurmountable obstacle.[310]

There are circumstances in which it might be bad policy, if not violative of other rights, to permit the focus of a record sole control over its dissemination. For example, a record written by or about person X might include descriptions of X's sexual abuse of a minor. It would be at the very least undesirable to give X carte blanche authority to consent to distribution of that record. While this might be a First Amendment issue, this should not be an issue for these Standards, because they concern law enforcement access, not public access, and there are restrictions on dissemination in Part VI.

(b) the focus of the record has knowingly and voluntarily given generalized consent to law enforcement access, and

- **(i) the information in the record is unprotected or minimally protected;**
- **(ii) it was possible to decline the generalized consent and still obtain the desired service from the provider requesting consent, and the focus of the record had specifically acknowledged that it was possible; or**
- **(iii) a legislature has decided that in a particular context, such as certain government contracting, generalized consent should suffice for the information contained in the record; or**

Commentary to Standard 25-5.1(b)

Standard 25-5.1(a) controls when the focus of a record consents to the specific law enforcement access immediately at issue. Whether an agreement with an institutional third party constitutes consent is more complicated. Whether or not they are recognized as such by contract law—which has very different purposes and incentive structures than

1997) (same); State v. Johnson, 346 A.2d 66, 68 (N.J. 1975) (same); State v. Trainor, 925 P.2d 818, 823 (Haw. 1996) (same for investigative encounter).

310. If there is an emergency, the government need not rely on consent. *See* Standard 25-5.4, *infra* p. 108.

the regulation of law enforcement investigations—we have all become accustomed to what are "take-it-or-leave-it" contracts of adhesion: we either "agree" to the terms of service, which may be dense, lengthy, and include a generalized permission for law enforcement access, or we cannot take advantage of that service. Meaningful bargaining is not only discouraged, but indeed is not possible. While such "take-it-or-leave-it" terms of service might be relevant to whether a third-party institution can decide on its own initiative and volition to provide information to law enforcement, that is a matter these Standards do not address.[311]

On the other hand, law enforcement may wish to take advantage of a third party consent just as could a private business desiring access to that information, and so long as the agreeing individual had a genuine choice, there is often no persuasive justification for not permitting law enforcement such access.[312] Moreover, with respect to information that is minimally protected according to Part IV (and thus necessarily also for information that is unprotected), the complexities of requiring a particularized contracting regime may not be worth the privacy gain.

Therefore, for highly protected and moderately protected information, a knowing and voluntary agreement with an institutional third party should only serve as consent to law enforcement access if the agreement was *individualized*, meaning the agreeing party knew he or she could refuse this permission and still take advantage of the desired service from this provider, and he or she specifically acknowledged this possibility. Perhaps the service was slightly more expensive in some manner absent this permission, but there was nonetheless a genuine option to refuse law enforcement access and still take advantage of the service. It would *not* be sufficient that the service was so available from a different provider; the agreeing party must know it was available from this very party seeking the generalized permission. And it would *not* be sufficient if this availability was buried in a click-through agreement or other lengthy agreement. By "specifically acknowledge," the Standards mean to require that the agreeing party separately acknowledged this option, for example by means of a second click-through that asked *solely* this question.

311. *See* Standard 25-2.1(f)(ii), *supra* p. 41.

312. This is not to say there is never such justification. *See, e.g.*, 18 U.S.C. § 2702(c) (permitting voluntary disclosure of certain non-content information to anyone other than the government).

For minimally protected and unprotected information, a knowing and voluntary agreement with an institutional third party that said institution can provide certain information to law enforcement constitutes consent according to the terms of that agreement. Law enforcement entities should nonetheless consider whether, as an internal administrative matter, there should be some oversight or restriction on such access of minimally protected information.

The discussion above concerns the rather impersonal contracting that pervades modern daily life, such as that required to open a financial or telecommunications account. There is of course also more individualized contracting, such as that required for employment. Although employers often possess significant amounts of very private information, such as that relating to matters of employee health, and despite employers often enjoying unequal bargaining power, in certain contexts it might nonetheless be appropriate to permit generalized consent to suffice despite the employee not having a choice to decline that consent and still obtain the employment. Thus, according to Standard 25-5.1(b)(iii), a legislature may decide in a particular context to render effective such a generalized consent.

(c) the record pertains to a joint account and any one joint account holder has given consent as provided in subdivision (a) or (b).

Commentary to Standard 25-5.1(c)

Consent should be required only from the person or persons who are the focus of the record as defined by Standard 25-1.1(c). For example, if law enforcement would like to obtain telephone call records for a particular telephone number, consent should only be required for the person owning that account, not from everyone with whom that owner thereby communicates. If the account is a joint account, as when two persons living together share a single telephone line, then the consent of either should suffice. But if the phone records of two unrelated accounts are requested, perhaps as a single merged record, consent should be required from each account holder. A person can only consent to the release of records relating to him or her, and not to those relating to others.

Using the examples from Standard 25-1.1(c), Bob has checking account number 312437 with a bank, and John and Joan Smith have joint checking account number 412835 with the bank. If the government wishes to

obtain the account balance for account 312437, Bob is the focus of the record, and therefore only Bob need consent. If the government wishes to obtain the account balance for account 412835, John and Joan are the focus of the record, but it is a joint account, so either the consent of John or the consent of Joan should suffice. If the government wishes to obtain the account balance for accounts 312437 and 412835 in a single document, Bob, John, and Joan are the focus of the record, and therefore the consent of Bob and either the consent of John or Joan should suffice.

Despite the language of this Standard, it might be the case, in rare circumstances, that a legislature might decide to require "all party consent" for records like some states require in the communications eavesdropping context. Because this will be rare, however, it is not accounted for in the black letter.

Finally, it might be worth noting that the constitutional decision in *Georgia v. Randolph*[313] does not require a more restrictive rule for access to records of joint accounts. In the records context there will almost never be a *physically present* objecting record holder, and *Randolph* is a narrow opinion in the context of the home that might well have no applicability outside of the home.[314]

Standard 25-5.2 Types of authorization

When authorization for accessing a record is required pursuant to Standard 25-5.3, it should consist of one of the following, each of which must particularly describe the record to be obtained:

(a) a *court order*, based upon:

313. 547 U.S. 103 (2006).

314. *See id.* at 121 (restricting the holding to a physically present objector); United States v. Hudspeth, 518 F.3d 954 (8th Cir. 2008) (en banc) (refusing to apply *Randolph* to a non-physically present objector); United States v. McKerrell, 491 F.3d 1221 (10th Cir. 2007) (refusing to apply *Randolph* where the would-be objector was not asked); Donald v. State, 903 A.2d 315 (Del. 2006) (same); United States v. DiModica, 468 F.3d 495 (7th Cir. 2006) (same); United States v. Groves, 530 F.3d 506 (7th Cir. 2008) (refusing to apply *Randolph* when the objector was no longer present); United States v. Henderson, 536 F.3d 776 (7th Cir. 2008) (refusing to apply *Randolph* when police caused the objector to no longer be present); United States v. King, 604 F.3d 125 (3d Cir. 2010) (refusing to apply *Randolph* to the seizure of a computer within the home). *But see* United States v. Murphy, 516 F.3d 1117 (9th Cir. 2008) (disagreeing with *Groves*, *Henderson*, and *King*).

(i) a judicial determination that there is probable cause to believe the information in the record contains or will lead to evidence of crime;
(ii) a judicial determination that there is reasonable suspicion to believe the information in the record contains or will lead to evidence of crime;
(iii) a judicial determination that the record is relevant to an investigation; or
(iv) a prosecutorial certification that the record is relevant to an investigation.

Commentary to Standard 25-5.2(a)

This Standard articulates the different types of authorization that might be used to regulate law enforcement access to third party records (organized from the greatest restraint to the least), and Standard 25-5.3 articulates which particular type should be required to access a given record.

Standard 25-5.2(a)(i) is the familiar warrant supported by probable cause required for many searches by the Fourth Amendment. As articulated by the Supreme Court, "[p]erhaps the best that can be said generally about the required knowledge component of probable cause . . . is that it raise a 'fair probability,' or a 'substantial chance,' of discovering evidence of criminal activity."[315]

The extent of information that can be obtained—often measured by temporal duration—is limited by that requisite suspicion. For example, imagine probable cause were required to obtain telephone and medical records. If there were probable cause to believe a person recently telephoned an accomplice, or placed a mobile phone call from within the vicinity of a recent crime, that would *not* indicate a fair probability that phone records dating from a year ago contain evidence of crime. Similarly, if there were probable cause to believe a person recently received treatment for a defensive wound, that would not indicate a fair probability that dated childhood medical records contain evidence of crime.

315. Safford Unified School District #1 v. Redding, 557 U.S. 364, 129 S. Ct. 2633, 2639 (2009) (citations omitted).

Standard 25-5.2(a)(ii) is a court order requiring a judge to find reasonable suspicion, once again a familiar Fourth Amendment standard. Although this substantive standard most often applies to limited protective searches like those authorized by *Terry v. Ohio*[316] and its progeny, it also governs evidentiary searches in "special needs" contexts like that of the public school.[317] The Supreme Court has defined reasonable suspicion as requiring a "moderate chance" of finding evidence of crime.[318]

Fourth Amendment searches authorized upon reasonable suspicion do not require ex ante approval by a court, but on account of the Fourth Amendment's exclusionary rule, prosecutors and courts are very familiar with evaluating ex post whether reasonable suspicion existed. Moreover, increasingly courts and prosecutors will have experience with court orders requiring reasonable suspicion, as, among other uses,[319] this is the developing standard for so-called "nontestimonial identification orders" requiring that a suspect undergo an identification procedure.[320] As with a Standard 25-5.2(a)(i) warrant, the amount of information requested must be considered in determining whether there exists the requisite reasonable suspicion.

Standard 25-5.2(a)(iii) is a court order requiring a judge to find the lesser quantum of relevance. Because a judge is making that substantive decision, this authorization requirement is more demanding than

316. 392 U.S. 1 (1968).

317. *See Safford*, 129 S. Ct. at 2639.

318. *Id.* at 2639. In the school context, not only evidence of crime is relevant but more broadly evidence of "wrongdoing," since administrators are not only enforcing law but also school rules. *Id.*

319. *See, e.g.*, 18 U.S.C. § 2703(d) (requiring "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").

320. *See, e.g.*, N.C.G.S.A. §§ 15A-271, 15A-273 (requiring prosecutor demonstrate probable cause that a sufficiently serious crime has been committed and "reasonable grounds" to suspect the person for which the identification procedure is requested); State v. Pearson, 356 N.C. 22, 28 (2002) (equating "reasonable grounds" with Fourth Amendment reasonable suspicion). *See also* Bousman v. Iowa Dist. Ct., 630 N.W.2d 789, 796-97 (Iowa 2001) (adopting same interpretation of identical statutory language); *In re* Nontestimonial Identification Order Directed to R.H., 762 A.2d 1239, 1242 (Vt. 2000) (same); State v. Cootz, 718 P.2d 1245, 1248 (Idaho Ct. App. 1986) (same); People v. Madson, 638 P.2d 18, 31-32 (Colo. 1981) (same).

Standard 25-5.2(a)(iv), according to which a judge must issue the court order upon a prosecutorial certification of relevance.

(b) a *subpoena*, based upon a prosecutorial or agency determination that the record is relevant to an investigation; or

Commentary to Standard 25-5.2(b)

This Standard uses the same substantive relevance criterion as the court orders of Standard 25-5.2(a)(iii) and 25-5.2(a)(iv), but is less demanding because a court need not be consulted. However, in accordance with Standard 25-5.3(a)(iii), a legislature wishing to permit a prosecutor or agency to directly access minimally protected information will have to provide appropriate subpoena authority.

(c) an *official certification*, based upon a written determination by a politically accountable official that there is a reasonable possibility that the record is relevant to initiating or pursuing an investigation.

Commentary to Standard 25-5.2(c)

This Standard uses the familiar criterion for evaluating grand jury subpoenas discussed in Standard 25-2.1(c). An official certification, meant to provide only a moderate measure of political accountability, is used in accessing de-identified records (Standard 25-5.6) and in disclosing already accessed records to another government agency (Standard 25-6.2(b)). Although an official certification should be written in order to further accountability, a digital writing can suffice. "Politically accountable official" is defined in Standard 25-1.1(f).

Standard 25-5.3 Requirements for access to records

(a) Absent more demanding constitutional protection, consent pursuant to Standard 25-5.1, and emergency aid and exigent circumstances pursuant to Standard 25-5.4; and consistent with the privilege requirements of Standard 5.3(c); law enforcement should be permitted to access a record maintained by an institutional third party pursuant to the following authorization:

(i) a court order under 5.2(a)(i) if the record contains highly protected information;

(ii) a court order under 5.2(a)(ii) [5.2(a)(iii) or 5.2(a)(iv)] if the record contains moderately protected information; or

(iii) a subpoena under 5.2(b) if the record contains minimally protected information.

Commentary to Standard 25-5.3(a)

This Standard articulates what regulation should be placed upon law enforcement access to a record according to the privacy of the information contained therein, as decided according to Part IV. The Standard applies when all of the following are true:

1. There is not a more demanding constitutional protection (see Standard 25-2.2);

2. There is not consent (see Standard 25-5.1);

3. There is no recognized exigency (see Standard 25-5.4); and

4. The information contained in the record is not protected differently by the law of privilege (see Standard 25-5.3(c)).

If the Standard applies, law enforcement should be required to:

i. Obtain a warrant to access a record containing highly protected information (Standard 25-5.3(a)(i));

ii. Obtain a lesser court order (one based on reasonable suspicion or relevance) to access a record containing moderately protected information (Standard 25-5.3(a)(ii)); and

iii. Obtain a non-judicial subpoena to access a record containing minimally protected information (Standard 25-5.3(a)(iii)).

For access to a record containing moderately protected information, Standard 25-5.3(a)(ii) permits a decision maker to choose from three different types of court order. It might select one option for certain types of moderately protected information, and another for different types of moderately protected information. Similarly, under Standard 25-5.3(a)(iii), a decision maker might require prosecutorial determination of relevance for certain minimally protected information and allow administrative determination to suffice for other minimally protected

information. In either case, a legislature will need to ensure that the prosecutor or administrative agency already has or is given the required subpoena authority.

(b) If the record contains highly protected information, a legislature, a court acting in its supervisory capacity, or an administrative agency could consider more demanding restraints for access to the record, such as additional administrative approval, additional disclosure, greater investigative need, or procedures for avoiding access to irrelevant information.

Commentary to Standard 25-5.3(b)

Under both the applicable ABA Criminal Justice Standards and federal law, more is required for law enforcement to intercept communications content than a warrant supported by probable cause: high-ranking administrative approval,[321] additional disclosure (both in the application[322] and ex post[323]), greater investigative need (both in the sense of magnitude of suspected crime[324] and the need for this particular investigatory technique[325]), and minimization procedures for avoiding access to irrelevant information.[326] Although employing the full panoply of such protections is likely to be very rare, a decision maker could consider such additional restraints in regulating law enforcement access to records containing highly protected information.

(c) The protections afforded to privileged information contained in records maintained by institutional third parties and the responsibilities of privilege holders to assert those privileges are those provided

---

321. *See* ABA Standards for Criminal Justice, *Electronic Surveillance, Section A: Electronic Surveillance of Private Communications* Standard 2-4.1(b) (3d ed. 2001); 18 U.S.C. § 2516.

322. *See* ABA Standards, *Electronic Surveillance, Section A*, *supra* note 321 Standard 2-4.2; 18 U.S.C. §§ 2518(1), 2518(2).

323. *See* ABA Standards, *Electronic Surveillance, Section A*, *supra* note 321 Standards 2-4.6(b)(iii), 2-4.15, 2-4.17; 18 U.S.C. §§ 2518(6), 2518(8)(d), 2519.

324. *See* ABA Standards, *Electronic Surveillance, Section A*, *supra* note 321 Standard 2-4.4; 18 U.S.C. §§ 2516, 2518(3)(a).

325. *See* ABA Standards, *Electronic Surveillance, Section A*, *supra* note 321 Standards 2-4.2(a)(xi), 2-4.3(c); 18 U.S.C. §§ 2518(c), 2518(3)(c).

326. *See* ABA Standards, *Electronic Surveillance, Section A*, *supra* note 321 Standards 2-2.1(d), 2-4.6(b)(v), 2-4.8(j), 2-4.9; 18 U.S.C. § 2518(5).

by the law applicable in the jurisdiction in which privilege is asserted. The jurisdiction in which law enforcement obtains documents may impose obligations on both institutional third parties to protect what might be privileged information and on law enforcement with respect to the access to, and storage and disclosure of, such information.

Commentary to Standard 25-5.3(c)

Like other ABA Criminal Justice Standards, these Standards recognize that special care and consideration may be appropriate in regulating access to privileged information.[327] Depending upon federal and state law, a non-exhaustive list might include accountant-client information,[328] attorney-client information,[329] priest-penitent information,[330] physician-patient information,[331] journalist-source information,[332] husband-wife information,[333] parent-child information,[334] and psychotherapist-patient information.[335] Rather than attempt a summary of that independent body of law, the Standards merely recognize its significance and incorporate its ramifications.

327. *E.g.*, ABA Standards, *Electronic Surveillance, Section A*, *supra* note 266 Standard 2-4.12. *See also*18 U.S.C. § 2517(4) ("No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.").

328. *See* 1 Am. Jur. 2d Accountants §§ 9-11.

329. *See* 81 Am. Jur. 2d Witnesses §§ 325-415; Jack B. Weinstein & Margaret A. Berger, Weinstein's Evidence Manual §§ 18.02A-18.03; 1 Jack B. Weinstein & Margaret A. Berger, Weinstein's Federal Evidence §§ 502.01-502.10; 3 Jack B. Weinstein & Margaret A. Berger, Weinstein's Federal Evidence §§ 503.01-503.44.

330. *See* 81 Am. Jur. 2d Witnesses §§ 493-504; 3 Jack B. Weinstein & Margaret A. Berger, Weinstein's Federal Evidence §§ 506.01-506.10.

331. *See* 81 Am. Jur. 2d Witnesses §§ 416-492; Jack B. Weinstein & Margaret A. Berger, Weinstein's Evidence Manual § 18.10; Jack B. Weinstein & Margaret A. Berger, 3 Weinstein's Federal Evidence §§ 514.01-514.14.

332. *See* 81 Am. Jur. 2d Witnesses §§ 525-531.

333. *See* 81 Am. Jur. 2d Witnesses §§ 284-324; Jack B. Weinstein & Margaret A. Berger, Weinstein's Evidence Manual § 18.05; 3 Jack B. Weinstein & Margaret A. Berger, Weinstein's Federal Evidence §§ 505.01-505.15.

334. *See* 81 Am. Jur. 2d Witnesses §§ 519-521.

335. *See* Jack B. Weinstein & Margaret A. Berger, Weinstein's Evidence Manual § 18.04; 3 Jack B. Weinstein & Margaret A. Berger, Weinstein's Federal Evidence §§ 504.01-504.09.

(d) Law enforcement should be permitted to access unprotected information for any legitimate law enforcement purpose.

Commentary to Standard 25-5.3(d)

A record containing unprotected information is subject to a minimal investigative restraint, but only that it be acquired for a legitimate law enforcement purpose. Although typically a law enforcement officer will acquire information only if he or she believes there is a reasonable possibility that it contains information relevant to an investigation, officers will also access unprotected information in order to stay informed regarding *potential* needs—such as learning of any community or public gathering that might require law enforcement assistance. "Legitimate law enforcement purpose" should be read broadly to permit such access.

The relevant language in the Attorney General Guidelines for Domestic FBI Operations provides as follows:

> All activities under these Guidelines must have a valid purpose consistent with these Guidelines, and must be carried out in conformity with the Constitution and all applicable statutes, executive orders, Department of Justice regulations and policies, and Attorney General guidelines. These Guidelines do not authorize investigating or collecting or maintaining information on United States persons solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution or laws of the United States.[336]
>
> * * *

336. The Attorney General's Guidelines for Domestic FBI Operations § I(C)(3) at 13, available at http://www.usdoj.gov/ag/readingroom/guidelines.pdf (last visited July 2, 2012). The introduction provides this further explanation:

> The general objective of these Guidelines is the full utilization of all authorities and investigative methods, consistent with the Constitution and laws of the United States, to protect the United States and its people from terrorism and other threats to the national security, to protect the United States and its people from victimization by all crimes in violation of federal law, and to further the foreign intelligence objectives of the United States. At the same time, it is axiomatic that the FBI must conduct its investigations and other activities in a lawful and reasonable manner that respects liberty and privacy and avoids unnecessary intrusions into the lives of law-abiding people.

> 1. The FBI is authorized to conduct investigations to detect, obtain information about, and prevent and protect against federal crimes and threats to the national security and to collect foreign intelligence, as provided in Part II of these Guidelines.
>
> 2. The FBI is authorized to provide investigative assistance to other federal agencies, state, local, or tribal agencies, and foreign agencies as provided in Part III of these Guidelines.
>
> 3. The FBI is authorized to conduct intelligence analysis and planning as provided in Part IV of these Guidelines.
>
> 4. The FBI is authorized to retain and share information obtained pursuant to these Guidelines as provided in Part VI of these Guidelines.[337]

(e) Law enforcement should be permitted to substitute a more demanding authorization for a required lesser authorization.

Commentary to Standard 25-5.3(e)

In an individual case, law enforcement should be permitted to substitute a greater authorization than is legally required. Thus, for example, subject only to Standard 25-5.3(b), a Standard 25-5.2(a)(i) court order could be used to obtain any record information. There can be various reasons why law enforcement may wish to substitute a greater authorization, perhaps foremost among them being convenience when such authorization is already required on account of other desired information.

The authorization requirements in Standard 25-5.2 are ordered from the greatest restraint to the least.

> The purpose of these Guidelines, therefore, is to establish consistent policy in such matters. They will enable the FBI to perform its duties with effectiveness, certainty, and confidence, and will provide the American people with a firm assurance that the FBI is acting properly under the law.

Id. at 5.

337. *Id.* § I(B) at 12.

Standard 25-5.4 Emergency aid and exigent circumstances

Law enforcement should be permitted to access a protected record for emergency aid or in exigent circumstances pursuant to the request of a law enforcement officer or prosecutor. As soon as reasonably practical, the officer or prosecutor should notify in writing the party or entity whose authorization would otherwise have been required under Standard 25-5.3.

Commentary to Standard 25-5.4

The preeminent function of law enforcement is to save life, and therefore these Standards permit a record sought for emergency aid (defined in Standard 25-1.1(a)) to be obtained upon officer or prosecutor request. Similarly, in order to avoid jeopardizing an investigation or prosecution, the Standards permit a record sought in exigent circumstances (defined in Standard 25-1.1(b)) to be obtained upon such request.

Because these Standards take no position on the exclusionary rule,[338] they take no position as to what remedy should ultimately be available if any of the following take place: (1) records were obtained purportedly for emergency aid where there was not reasonably believed to be imminent danger of death or serious physical injury; (2) records were obtained purportedly for reasons of exigency when there was not probable cause to fear imminent destruction of evidence or imminent flight; or (3) records were obtained for reasons of exigency when the authorization required by Standard 25-5.3 could not have been obtained had there been no exigency. More generally, Standard 25-7.1 leaves the framing of appropriate sanctions to the legislature.

Because this Standard permits records access upon officer or prosecutor request that would ordinarily require perhaps a warrant or other court order, this Standard provides a mechanism for accountability and guidance. Although the drafters considered requiring ex post review of the triggering circumstance in every instance, there was a concern that such a requirement would overly burden law enforcement. Therefore, the Standard provides that the requesting officer or prosecutor should notify, but not necessarily receive a substantive review from, the party

338. *See* Standard 25-7.1, *infra* p. 131.

or entity that would typically authorize the particular record access under Standard 25-5.3.

Unlike the warrantless entry to a home, which officers can undertake without assistance when legally permitted, access to records will often require the cooperation of a third party. Therefore, legislatures should consider whether to require that a third party cooperate with a Standard 25-5.4 request upon some sort of certification, and whether to immunize third parties that so respond in good faith.

Standard 25-5.5 Redacted access to records

Legislatures, courts that may act in a supervisory capacity, and administrative agencies should consider how best to regulate:

(a) law enforcement access when only some information in a record is subject to disclosure; and

Commentary to Standard 25-5.5(a)

In a physical search, such as that of a home, a law enforcement officer often sorts through a great deal of irrelevant and potentially private information in order to find what he or she is lawfully seeking: in general, an officer may look anywhere a sought-after item could be. This is acceptable both because there is no realistic alternative and because a warrant is typically required for the search. In the case of access to third party records, there is an alternative, namely to require the third party to conduct that search.[339] And, as made clear in Standard 25-5.3(a) and existing law, a warrant will often not be required for records access.

To be clear, there are two "layers" of relevant search. First, a record may contain whole categories of information that law enforcement is either not permitted to access or is not choosing to access, such as financial transaction information when law enforcement only wants cumulative account details. Here decision makers should strongly consider requiring the third party to conduct this redaction, perhaps being com-

339. *See* United States v. Bach, 310 F.3d 1063 (8th Cir. 2002) (permitting third party employees to conduct search); 18 U.S.C. § 2703(g) (same). Of course, if the third party is itself a suspect, this would not be a meaningful alternative.

pensated therefore by the law enforcement entity making the request.[340] If that is not feasible, it might be reasonable to require an independent special master, or a taint team within law enforcement such that only the permitted information is reviewed by those conducting the relevant investigation. Second, a record will typically contain significant irrelevant information of the very type being requested—for example, innocent financial transactions among those indicative of criminal activity. Here the norm would be to permit law enforcement to itself make this substantive separation.

Because there are not yet established norms among the many different content types and different jurisdictions, these Standards do not take a substantive position on these matters in the black letter.

(b) the use and dissemination of information by law enforcement when a third party provides more information, including more protected information, than was requested.

Commentary to Standard 25-5.5(b)

As discussed with respect to Standard 25-5.5(a), the third party will have at least some role—and potentially a significant role—in separating out responsive information that will then be conveyed to law enforcement. It will sometimes happen that the third party thus mistakenly provides information. For example, a phone company might provide three days of telephone dialing information when only two days of data was requested. Or, that phone company might provide stored voicemails when only dialing information was requested. Although in the national security context, a relevant data point is a report by the Department of Justice Inspector General's Office that found a mistake was made in 7.5% of the National Security Letters it sampled: half were errors on the part of the third party providing the requested information.[341]

These Standards take no position on the suppression of evidence,[342] and therefore take no position on whether such information should be

340. *See, e.g.*, 18 U.S.C. § 3124(c) (requiring reasonable compensation in the context of a pen trap); 18 U.S.C. § 2706 (requiring reimbursement in the context of stored communication records).

341. *See* Richard Brust, *Letters of the Law*, ABA Journal, Sept. 2012, at 71.

342. *See* Standard 25-7.1.

admissible.[343] Decision makers should consider, however, not only this ultimate evidentiary issue but also how law enforcement should be required to respond. One might imagine a distinction between mistakes a reasonable officer would not notice—such as a minor deviation in duration of records—and a mistake a reasonable officer would notice—such as a major deviation in duration or a deviation in type of information. If any potential liability is placed upon third parties in order to encourage their due care, it could also positively incentivize that care by providing an appropriate safe harbor.

Standard 25-5.6 De-identified records

(a) Notwithstanding any other provision of this Part, law enforcement should be permitted to access an appropriately inclusive body of de-identified records maintained by an institutional third party pursuant to an official certification.

(b) A de-identified record should be linked to an identifiable person only if law enforcement obtains the authorization required under Standard 25-5.3 for the type or types of information involved. The showing for this authorization may be based on a profile or algorithm.

Commentary to Standard 25-5.6

There will be circumstances in which law enforcement would be unable to satisfy the access requirements of Standard 25-5.3 because it lacks individualized suspicion, but in which there remains a legitimate law enforcement purpose in accessing a large group of private records to detect crime. For example, it might be possible to discern fraud from a pattern of health care or automobile accident claims, to detect drug or human smuggling from toll tag and other records, or to determine the identity of a serial bank robber from cell phone location records.

On the one hand, this is perhaps a lesser intrusion. As in the non-record context of an automobile roadblock, each person can take solace in knowing that he or she is not individually under suspicion. On the other hand, it is a greater intrusion, in that persons whose records

343. *See, e.g.*, State v. Canady, 161 Wash. App. 1009, 2011 WL 1459733 (Wash. Ct. App. 2011) (unpublished) (refusing to suppress text messages outside the scope of the warrant).

would never otherwise come to the attention of law enforcement are now perused.[344] In order to accommodate these competing interests, these Standards permit law enforcement access to appropriately inclusive bodies of *de-identified* records, but permit linkage to an identifiable person only upon a requisite showing of suspicion.

Such acquisition is limited to an "appropriately inclusive" body of records because, in combination with the notice requirements of Standard 25-5.7(e), broad and uniform applicability provides a "political process check": There will be a more spirited debate and presumably effective oversight when those in positions of power and influence are subjected to an intrusion. When confronted with student drug testing, the Supreme Court recognized that a broader search might in certain circumstances be preferable to a narrower one,[345] and Professor William Stuntz has argued this point: "[S]preading the cost of policing through a larger slice of the population . . . reduces the odds of voters demanding harsh and intrusive police tactics secure in the knowledge that those tactics will be applied only to others."[346] Yet criticisms of this doctrine also draw blood. In another context, Justice William Rehnquist derided it as a jurisprudence of "misery loves company,"[347] and in the school drug context dissenting justices argued that "[b]lanket searches, because they can involve thousands or millions of searches, pose a greater threat

344. The Department of Defense's Technology and Privacy Committee thus concluded that "[s]earches that lack specific focus on identified suspects . . . pose greater risks for U.S. persons and should be subject to greater scrutiny and accountability." TAPAC, *Safeguarding Privacy in the Fight Against Terrorism* 45 (2004), available at http://www.defenselink.mil/news/Jan2006/d20060208tapac.pdf (last visited June 13, 2012). Even courts that have rejected constitutional restraints upon limited government surveillance have recognized a larger concern with dragnet surveillance, one interpretation of which is surveillance applied indiscriminately to the masses. *See, e.g.*, United States v. Knotts, 460 U.S. 276, 283-84 (1983) (vehicle location tracking); United States v. Garcia, 474 F.3d 994, 997-98 (7th Cir. 2007) (same).

345. *See* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 664 (1995).

346. William Stuntz, *Local Policing After Terror*, 111 Yale L.J. 2137, 2166 (2002). *See also* William J. Stuntz, *Implicit Bargains, Government Power, and the Fourth Amendment*, 44 Stan. L. Rev. 553, 588 (1992) ("Fourth Amendment regulation is usually unnecessary where large numbers of affected parties are involved. Citizens can protect themselves in the same way that they protect themselves against most kinds of government misconduct–they can throw the rascals out."); Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 Mercer L. Rev. 507, 554-59 (2005).

347. Delaware v. Prouse, 440 U.S. 648, 664 (1979) (Rehnquist, J., dissenting).

to liberty than do suspicion-based ones, which affect one person at a time."[348]

But when combined with so-called "selective revelation," permitting these broader records searches upon a lesser threshold is an effective compromise. Selective revelation permits a broad search, but reveals personally identifiable information only if that initial search demonstrates the requisite suspicion. For example, although arguably most such searches are typically best left to the private sector, perhaps law enforcement would search large de-identified databases of mortgage records for anomalies indicative of fraud. Or, perhaps the search would be of a large body of cell phone location records to determine whether a single phone was located near each of a number of robberies.[349] If there were no "hits," that would be the end of the matter, and the data would be destroyed (or, even better, the data would never leave the institutional third party if the search could be run directly on its systems). If there were positive hits, law enforcement would be authorized to identify and inspect the specified records only upon satisfying the ordinary standard for accessing, respectively, financial transaction records or cell phone location records. The fact of a hit could itself satisfy this standard if the algorithm were provably effective,[350] and in this case it might be necessary to retain the entire database until all relevant investigation and litigation, including any post-conviction appeals, is complete (see Standard 25-6.1(c)).

In the words of the Defense Advanced Research Projects Agency ("DARPA") Information Science and Technology Study Group on Security and Privacy,

> The idea of selective revelation is that initially we reveal information to the analyst only in sanitized form, that is, in terms of statistics and categories that do not reveal

348. *Vernonia*, 515 U.S. at 667 (O'Connor, Stevens, Souter, J.J., dissenting).

349. *See, e.g.*, Larry Hendricks, 18 Years in Prison for High Country Bandit, Arizona Daily Sun, June 6, 2012, available at http://azdailysun.com/news/local/crime-and-courts/years-in-prison-for-high-country-bandit/article_1b1634ee-8909-55de-bf87-8e3962e29eaf.html (last visited July 2, 2012) (describing successful investigation of bank robbers that began with cell phone records).

350. To the extent algorithms have quantified reliability, it might be helpful for lawmakers to set more precise thresholds than the vague quanta of suspicion we typically use (e.g., reasonable suspicion and probable cause). *See* Erica Goldberg, *Getting Beyond Intuition in the Probable Cause Inquiry*, Lewis & Clark L. Rev. (forthcoming).

> (directly or indirectly) anyone's private information. If the analyst sees reason for concern he or she can follow up by seeking permission to get more precise information. This permission would be granted if the initial information provides sufficient cause to allow the revelation of more information, under appropriate legal and policy guidelines.
>
> For example, an analyst might issue a query asking whether there is any individual who has recently bought unusual quantities of certain chemicals, and has rented a large truck. The algorithm could respond by saying yes or no, rather than revealing the identity of an individual. The analyst might then take that information to a judge or other appropriate body, seeking permission to learn the individual's name, or other information about the individual. By revealing information iteratively, we prevent the disclosure of private information except when a sufficient showing has been made to justify that revelation.[351]

The most secure manner of selective revelation would be to require a computer architecture which would not permit law enforcement officials to see any of the data, but which they could instruct to search that data for anomalies of interest and learn in response only whether or not there is a hit. Smaller police departments, however, will not have the funds necessary to commission the creation of such an architecture, off-the-shelf systems may or may not provide the requisite selective revelation and might be similarly expensive,[352] and institutional third parties may often have no motivation to themselves create such a system. Therefore, these Standards permit a form of selective revelation via de-identification. The government works only with the de-identified data unless and until it has satisfied the relevant requirements of Standard 25-5.3, in which case it can re-identify those particular records.

---

351. Report from the Information Science and Technology Study Group on Security and Privacy, *Security with Privacy*, Dec. 2002, at 10, available at http://www.eecs.berkeley.edu/~tygar/papers/ISAT-final-briefing.pdf (last visited July 2, 2012).

352. For an example of such a data mining system, see Palantir, palantir.com (last visited July 2, 2012); Shane Harris, *Killer App: Have a Bunch of Silicon Valley Geeks Figured Out How to Stop Terrorists?*, Washingtonian, Feb. 2012, at 71, available at http://palantir.com/_ptwp_live_ect0/wp-content/uploads/2012/03/WashingtonianArticle2.pdf (last visited July 2, 2012).

For a discussion on the science of de-identification, and potential complications therein, see Standard 25-1.1(g). While it is not necessary to repeat that material here, it is important to emphasize that decision makers should proceed with caution. The science is complicated, both in de-identifying data and in algorithms that would detect suspicious activity. If there are doubts about either, law enforcement can be required to satisfy them before any transfer of data takes place.

At the same time, legislatures may want to think broadly about how to achieve the purposes of this Standard. For example, in 2005, police in Rotterdam, Netherlands, wanted to identify those involved in a riot.[353] So, from phone providers they obtained the 17,000 mobile telephone numbers corresponding to phones known to be in the vicinity. Police sent a text message to every number, requesting that anyone with information on the riots contact the police. The police then deleted the database of numbers.[354] It would be important that the message convey its "appropriately inclusive" breadth. For example, it might state as follows:

> Based on telephone provider records that we are using solely for this purpose (and our copy of which will be deleted once this is sent), we have reason to believe you were one of the thousands of persons near the Rotterdam riots on [whatever date]. If you have any information on the riots or on specific rioters, please contact the police at [contact information].

Assuming such a properly informative and nonthreatening message, this seems a smart investigatory tool that is respectful of privacy, and one that is within the spirit of these Standards.[355]

353. *See* Bruce Schneier, Schneier on Security 28 (2008).

354. The Standards require ultimate deletion of all de-identified records. *See* Standard 25-6.1(c).

355. The text message actually used by police may have lacked clarity. *See* David Rennie, *Dutch Soccer Riot Suspects Turn Themselves In After Receiving Text Message*, National Post, Sept. 1, 2005, at A14 (describing it as a "terse message . . . informing users they were known to have been in the vicinity").

Standard 25-5.7 Notice

(a) If the accessed record is unprotected or minimally protected, law enforcement should not be required to provide notice of the access.

(b) If the accessed record is highly or moderately protected, law enforcement should provide notice of the access to the focus of the record, and this notice should generally occur within thirty days after acquisition.

Commentary to Standard 25.5-7(a) and (b)

Providing notice of records access not only serves accountability, but provides the engines of democracy the information required for their deliberative functions.[356] Moreover, notice itself respects privacy. As discussed in the Commentary to Standard 25-3.3, at its core, information privacy concerns the ability to control what information about you is conveyed to others, and for what purposes. The apex of control, and therefore of privacy, is a complete absence of nonconsensual disclosures. But where that is impossible given competing interests in law enforcement, the next best option is to be informed about a disclosure. There is an ongoing harm from covert information gathering that continues until notice is provided. Only after notification does a person once again have the information necessary to make fully informed and rational choices.[357] Federal Magistrate Judge Stephen William Smith of the Southern District of Texas has expressed this concern regarding the current system's failure to provide notice of government surveillance requests: "Through a potent mix of indefinite sealing, nondisclosure (i.e.,

356. *See, e.g.*, Commentary to Standard 25-5.6, *supra* at p. 111.

357. *See* Stanley I. Benn, A Theory of Freedom 276 (1988) ("To protect [the target's] feelings by keeping him in ignorance of what was happening, so far from eliminating the injury . . ., would exacerbate it by the further insult of deliberately falsifying his self-perception."). Although in America we are fortunate to experience nothing like the totalitarian regime of the former East Germany, the unified government's ultimate decision to open the secret files of the East German Secret Police (commonly known as the Stasi), demonstrates an example of these principles. *See* Stephen Kinzer, *East Germans Face Their Accusers*, N.Y. Times Mag., April 12, 1992. Indeed, more than twenty years after the fall of the regime, Germans are still working to piece together the vast collection of hand-shredded Stasi documents, and tens of thousands of persons request to see the documents each year. *See* Philip Reeves, *Piecing Together 'The World's Largest Jigsaw Puzzle'*, NPR News, Oct. 8, 2012.

gagging), and delayed-notice provisions, [relevant federal statutory] surveillance orders all but vanish into a legal void. It is as if they were written in invisible ink—legible to the phone companies and internet service providers who execute them, yet imperceptible to unsuspecting targets, the general public, and even other arms of government, most notably Congress and the appellate courts."[358]

There is a competing consideration, namely the administrative burden that notice places upon law enforcement. Thus, these Standards do not require notice when accessed records contain unprotected or minimally protected information. But when accessed records contain highly or moderately protected information, the Standards require notice, and that notice should generally occur within thirty days after acquisition. Although in some circumstances law enforcement is accustomed to provided immediate notice of access (e.g., when executing a warrant,[359] issuing a subpoena directly to the target,[360] or seeking third party records relating to a victim of crime[361]), in others this will be a novel requirement.[362] Legislatures should therefore provide the necessary resources to comply, and law enforcement should develop and provide the necessary training. The thirty day period is intended to provide some flexibility in implementation, and to discourage what might otherwise be frivolous complaints of noncompliance.

There is of course also a risk to providing notice, in that information can be destroyed, witnesses can be intimidated, and investigations

358. Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 Harv. L. & P. Rev. 601, 602 (2012).

359. *See* Fed. R. Crim. P. 41(f)(1)(C); United States Courts, *Search and Seizure Warrant*, http://www.uscourts.gov/uscourts/FormsAndFees/Forms/AO093.pdf ("Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.") (last visited July 2, 2012); U.S. Department of Justice, *Delayed Notice Search Warrants: A Vital and Time-Honored Tool for Fighting Crime*, Sept., 2004, available at http://www.justice.gov/dag/patriotact213report.pdf (last visited July 2, 2012).

360. *See* United States v. Dionisio, 410 U.S. 1, 10 (1973). *See also* S.E.C. v. Jerry T. O'Brien, Inc., 467 U.S. 735 (1984) (restricting the required notice to the third party in the case of third party records).

361. *See* Fed. R. Crim. P. 17(c)(3).

362. Just as existing privacy law tends to be rather ad hoc and sectoral, so do existing notification requirements. *See, e.g.*, 12 U.S.C. §§ 3405(2), 3406(b), 3407(2), 3408(4)(A) (financial records); 18 U.S.C. § 2710(b)(3) (video rental records); 47 U.S.C. § 551(h)(2) (cable records).

can be otherwise impeded. Thus, Standard 25-5.7(c) and 5.7(d) permit delayed notification. Standard 25-5.7(f) more generally permits a court to limit notice in a particular instance in which that notice would be unduly burdensome.

Notice is required only to the focus of a record (defined in Standard 25-1.1(c)), not necessarily to every person mentioned in that record.[363] Thus, using the example from Standard 25-1.1(c)'s Commentary, Bob has checking account number 312437 with a bank, and John and Joan Smith have joint checking account number 412835 with the bank. Assuming financial account information is moderately or highly protected, and assuming a court order were used to obtain the account balance for account 312437, Bob is the focus of the record, and therefore notice should be provided to Bob but not to everyone with whom the records show he did business. If a court order were used to obtain the account balance or other account information for account 412835, John and Joan are the focus of the record, and therefore notice should be provided to both, even if that information strongly relates to only one of them (e.g., only John has written checks on the account). If a court order were used to obtain the account balance for accounts 312437 and 412835 in a single document, Bob, John, and Joan are the focus of the record, and therefore notice should be provided to all three.

Were consent limited to when the focus of a record has knowingly and voluntarily consented to a specific law enforcement request (Standard 25-5.1(a)), then notice would be unnecessary when law enforcement accesses a record via consent, arguably even in the joint account context. Because consent under these Standards extends to generalized consents (Standard 25-5.1(b)), access by means of consent is not carved out of this Standard's notification requirement.

(c) The court that authorizes access to the record, or in the case of emergency aid or exigent circumstances the court that would otherwise have been required to authorize access to the record, may delay notice for a specified period, or for an extension thereof, upon its determination that:

363. A statutory analog can be found in the Wiretap Act, which requires notice only to the person or persons named in the wiretap order, but includes a judicial opportunity to provide more extensive notice. *See* 18 U.S.C. § 2518(8)(d). For a skeptical view of this limitation, see James Carr & Patricia L. Bellia, 1 Law of Electronic Surveillance § 5:46 (2012).

(i) there is a reasonable belief that notice would endanger life or physical safety; would cause flight from prosecution, destruction of or tampering with evidence, or intimidation of potential witnesses; or would otherwise jeopardize an investigation; or
(ii) the delay is necessary to comply with other law.

Commentary to Standard 25-5.7(c)

While these Standards provide for a broad system of notice, they also recognize the potential need to delay that notice. This Standard tracks the language of many of the federal statutory delayed notice provisions,[364] and includes a catch-all where delay is necessary to comply with other law, such as where treaty obligations might require delaying notice where access is accomplished to benefit a foreign government.[365] The determination as to whether delay is appropriate is made by the entity that either is authorizing the access or that absent an exigency would typically authorize the access, which in the case of moderately or highly protected information will be a court (see Standard 25-5.3(a)).

(d) When a court authorizes delayed notice pursuant to Standard 5.7(c), the court may also prohibit the third party from giving notice during that specified period. If law enforcement obtains a record for emergency aid or in exigent circumstances, a law enforcement officer or prosecutor may by written demand prohibit the third party from giving notice for 48 hours.

Commentary to Standard 25-5.7(d)

This Standard dovetails with 25-5.7(c): if there is ample justification for delaying notice from law enforcement, there is ample justification for temporarily preventing the third party from itself providing such notice. Of course, Standard 25-5.7(b) provides a thirty-day window in which law enforcement can provide the required notice; if law enforcement wishes to prevent third party notice for, say, two weeks, it can use this same mechanism but will have to satisfy the Standard 25-5.7(c)

364. *See* 12 U.S.C. § 3409; 15 U.S.C. § 57b-2a; 15 U.S.C. § 1681b(b)(4); 18 U.S.C. § 983(a)(1)(D); 18 U.S.C. § 2705.
365. *See, e.g.*, 18 U.S.C. § 3512; 28 U.S.C. § 1782.

substantive requirements for delaying notice. In an exigent situation, the Standard provides 48 hours in which law enforcement can obtain the necessary court order.

(e) When protected de-identified records are accessed, notice should be provided to the [general public] [legislature] and should generally occur [prior to] [after] acquisition.

Commentary to Standard 25-5.7(e)

As explained in the Commentary to Standard 25-5.6, one of the important restraints on law enforcement access to bodies of de-identified records, which are otherwise far easier to obtain than their identified equivalents, is the "political process check" of informed debate and oversight. Thus, these Standards require notice for access to de-identified records that contain highly, moderately, or minimally protected information.

Arguably such informed debate is most effective if the interested public has advanced notice of the access, providing the opportunity for the political equivalent of a motion to quash. But effective accountability can also occur via ex post notice: if law enforcement is seen as abusing this access, a legislature can restrict it going forward. Thus, the Standard permits either option, allowing, for example, advanced notice via a publication like the Federal Register,[366] which at least in theory provides notice to the general public, or ex post notice via reporting to Congress.[367] In all, the Standard recognizes four options that a legislature might apply to law enforcement access to a particular type of de-identified information: prior notice to the general public, prior notice to the legislature, ex post notice to the general public, and ex post notice to the legislature.

(f) Upon request, a court should be permitted to eliminate or limit the required notice in a particular case where it would be unduly burdensome given the number of persons who must otherwise be

366. *See, e.g.*, 5 U.S.C. § 552a(e)(11) (provision of Privacy Act requiring that an agency must "at least 30 days prior to publication of information [regarding a system of records,] . . . publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency").

367. *See, e.g.*, 18 U.S.C. § 2519(3) (provision of Wiretap Act requiring annual reporting to Congress).

notified, taking into consideration, however, that the greater number of persons indicates a greater intrusion into privacy.

Commentary to Standard 25-5.7(f)

Even with requiring notice only for access to records containing moderately and highly protected information (Standard 25-5.7(a)), and despite requiring notice only to the focus of a record (Standard 25-5.7(b)), there may nonetheless be rare instances in which notice would be unduly burdensome because so large a number of persons would have to be notified. Although such broad law enforcement access to information is also potentially the most troubling, a court should be permitted to consider eliminating or limiting the required notice in order to account for the unusual and extreme administrative burden.

Part VI. Retention, Maintenance, and Disclosure of Records

Standard 25-6.1 Retention and maintenance

(a) Protected records lawfully obtained from an institutional third party in the course of law enforcement investigation should be:

Commentary to Standard 25-6.1(a)

An argument can be made that while law enforcement obviously must acquire records in order to fulfill its missions, it should often *not* archive, and generally not combine, those records lest it "result in the development, over time, of a massive government database."[368] However, competing considerations including the crime-fighting benefits of sharing information across many agencies, and indeed across the entire local, state, and federal law enforcement community, are leading to the creation of just such databases, such as the Federal Bureau of Investigation's Law Enforcement National Data Exchange ("N-DEx").[369] Whereas the National Crime Information Center ("NCIC") has long served as a clearinghouse for criminal record information,[370] N-DEx will include substantive data contained in federal, state, local, and tribal "incident, offense and case reports as well as arrest, booking, incarceration, and parole and/or probation information."[371]

It is therefore critical that decision makers not only regulate law enforcement access to records maintained by institutional third parties,

368. Markle Foundation Task Force on National Security in the Information Age, *Mobilizing Information to Prevent Terrorism: Accelerating Development of a Trusted Information Sharing Environment* 31 (2006), available at http://www.markle.org/sites/default/files/2006_nstf_report3.pdf (last visited July 2, 2012).

369. *See* http://www.fbi.gov/about-us/cjis/n-dex (last visited July 2, 2012); Notice to Establish New System of Records, 72 Fed. Reg. 56793 (Oct. 4, 2007).

370. *See* http://www.fas.org/irp/agency/doj/fbi/is/ncic.htm (last visited July 2, 2012); Notice of Modified System of Records, 64 Fed. Reg. 52343 (Sept. 28, 1999).

371. 72 Fed. Reg. at 56793.

but also regulate subsequent access to, and maintenance of, information so obtained. Although the restrictions in this Part address the disposition only of such records, they are meant to also apply to law enforcement manipulations of that data (e.g., data recast into a spreadsheet or other format).

Standard 25-6.1(a) refers only to records that are *lawfully* accessed by law enforcement because records accessed illegally should arguably be destroyed or returned. However, just as with respect to the trial exclusionary rule (see Standard 25-7.1), these Standards take no position on the disposition of illegally obtained data.

(i) reasonably secure from unauthorized access; and

Commentary to Standard 25-6.1(a)(i)

When law enforcement acquires private information, here in the form of a protected record maintained by an institutional third party, it takes on an obligation to keep it reasonably secure from unauthorized access, which requires appropriate administrative, physical, and technical safeguards. Administrative rules should restrict physical and electronic access to those with a need to know to perform their official duties, and comply with the other limitations of these Standards. To the extent possible, records and records access points should be physically segregated via locks and alarm devices, and all digital records should be password protected and transmissions thereof should be encrypted.

Decision makers can learn more about securing information, including detailed descriptions of administrative, physical, and technical safeguards, by consulting guides like these: NIST Special Publication 800-100, *Information Security Handbook: A Guide for Managers* (Oct. 2006);[372] NIST Special Publication 800-66 Revision 1, *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule* (Oct. 2008);[373] and NIST Special Publication

372. Available at http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf (last visited July 2, 2012).

373. Available at http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf (last visited July 2, 2012).

800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* (Aug. 2009).[374]

(ii) other than as authorized under Standard 25-6.2, accessed only by personnel who are involved in the investigation for which they were obtained and only to the extent necessary to carry out that investigation.

Commentary to Standard 25-6.1(a)(ii)

According to Part V of these Standards, records are to be accessed for a particular purpose and upon a particular justification. Nonetheless, records acquired for one purpose might later prove useful for another, and these Standards recognize and permit that flexibility via Standard 25-6.2.

(b) Moderately and highly protected records should in addition be:
(i) subject to audit logs recording all attempted and successful access; and

Commentary to Standard 25-6.1(b)(i)

Audit logs provide critical accountability, and whether records are retained in hardcopy or electronic form, logs should record who accesses the system, when, for what purpose, and what information was obtained. The periodic review of Standard 25-7.3 should include reviews of these logs in order to deter, detect, and investigate illegitimate use. Ideally, audit logs should be immutable: if they can be modified or erased, a malicious user can illegitimately access the system and then erase the evidence thereof. At the very least, those who maintain the logs should not be those who access the records. Where access is automated, computer code should prevent records from being accessed without leaving a proper audit trail; in all circumstances administrative regulations should do the same.

For more information on audit logs, including on how to avoid those logs themselves becoming a security risk, decision makers can consult security publications like these: NIST Special Publication 800-92,

374. Available at http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf (last visited July 2, 2012). Further relevant NIST publications are available at http://csrc.nist.gov/publications/PubsSPs.html (last visited July 2, 2012).

Guide to Computer Security Log Management (Sept. 2006);[375] NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, 50-53 (Sept. 1996);[376] Markle Task Force on National Security in the Information Age, *Implementing a Trusted Information Sharing Environment: Using Immutable Audit Logs to Increase Security, Trust, and Accountability* (Feb. 2006).[377]

(ii) destroyed according to an established schedule.

Commentary to Standard 25-6.1(b)(ii)

The utility of different types of data decreases at different rates of time, and the ability to preserve data will depend on very localized circumstances such as secure building space and electronic resources. While these Standards therefore do not recommend a specific period of retention, every agency should develop data destruction protocols as part of its overall data retention and maintenance plan. It is critical that when private data is no longer required, it be destroyed rather than merely discarded.

(c) All de-identified records in the possession of law enforcement for which the linkage described in Standard 5.6(b) is not obtained should be destroyed upon conclusion of the investigation and any prosecution and appeals.

Commentary to Standard 25-6.1(c)

As described in Standard 25-5.6 and its Commentary, these Standards permit a form of selective revelation in which law enforcement accesses an inclusive body of de-identified records, but re-identifies a record only if it obtains the requisite authorization. The downside of this method of investigation is that the records pertaining to a large number of innocent persons are necessarily perused, but that downside is manageable so long as those records are destroyed as soon as is possible without negat-

375. Available at http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf (last visited July 2, 2012).

376. Available at http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf (last visited July 2, 2012).

377. Available at http://www.markle.org/sites/default/files/nstf_IAL_020906.pdf (last visited July 2, 2012).

ing the very utility of the access. Thus, this Standard requires destruction upon conclusion of the investigation and any prosecution and appeals, potentially including post-conviction challenges.

Ideally, law enforcement would not acquire the de-identified records, but would instead search them while still in the possession and maintenance of the institutional third party. Because that may not be feasible in all circumstances, however, the Standards rely upon destruction of records as a second best alternative.

(d) If a law enforcement agency disseminates internal regulations pursuant to this Standard, those regulations should be publicly distributed.

Commentary to Standard 25-6.1(d)

Public dissemination of these regulations not only fosters accountability in its own right, but allows review and comment by those with technical or other security knowledge.

Standard 25-6.2 Disclosure and dissemination

Law enforcement should not disclose protected records to individuals and entities not involved in the investigation for which they were obtained except in the following circumstances:

(a) Disclosure in the case or cases investigated, pursuant to rules governing investigation, discovery and trial;

Commentary to Standard 25-6.2(a)

Dissemination of information during investigation and trial is governed by many sources, including constitutional law,[378] ethics codes,[379] other American Bar Association Standards,[380] and statutes and rules of procedure.[381] It is not the intent of these Standards to alter or summarize that diverse material, but rather to make clear that disclosure of infor-

378. *E.g.*, Gentile v. State Bar of Nevada, 501 U.S. 1030 (1991).

379. *E.g.*, ABA Model Rules of Prof'l Conduct R. 3.6 (2009).

380. *E.g.*, ABA Standards for Criminal Justice, *Prosecutorial Investigations* Standard 1.5 (2008 in black letter).

381. *E.g.*, Fed. R. Crim. P. 6; 28 C.F.R. § 50.2.

mation contained in law enforcement records should be governed by those rules and hortatory principles.

(b) Disclosure for purposes of other government investigations, including parallel civil investigations, unless prohibited by law, and except that such disclosure to another government agency should require official certification or, in the case of emergency aid or exigent circumstances, the request of a law enforcement officer or prosecutor;

Commentary to Standard 25-6.2(b)

Among other means of access, the federal Privacy Act permits a government agency to disclose a record to another agency if the "head of the [requesting] agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought."[382] These Standards likewise permit disclosure for legitimate law enforcement purposes unrelated to the original access, including disclosure to other law enforcement agencies engaged in their enforcement responsibilities and to private persons as a necessary incident to that enforcement (e.g., information provided to encourage a potential witness). As in the Privacy Act, however, such inter-agency access should be regulated. Absent emergency aid or exigent circumstances, it should require official certification as that term is defined in Standard 25-5.2(c).

For example, if an Arizona Department of Public Safety ("DPS") officer would like to obtain a record previously obtained from an institutional third party by the Colorado Bureau of Investigation, that access should be permitted upon a written determination by a politically accountable official within the Arizona DPS that there is a reasonable possibility that the record is relevant to initiating or pursuing an investigation. This substantively minimal requirement provides a measure of political accountability for such inter-agency transfers. It should be noted that the record could be relevant to pursuing *or initiating* an investigation. Thus, if the Colorado Bureau of Investigation itself believes a record might be relevant to opening a new investigation in Arizona, a politi-

382. 5 U.S.C. § 552a(b)(7).

cally accountable official of the Bureau of Investigation can provide the required certification.

Because the necessary law enforcement information sharing can sometimes only practically take place if the information has previously been stored in an accessible database, nothing in these Standards is meant to prohibit such combination of records, including among different agencies and departments, so long as that database comports with these Standards. Thus, if an officer with the Arizona DPS wants to access a database containing records from law enforcement investigations in Colorado, an official certification would be required in the absence of emergency aid or exigent circumstances.

(c) Disclosure with appropriate redaction for purposes of training, auditing, and other non-investigatory legitimate law enforcement purposes only upon a written determination by a politically accountable law enforcement official that the access is in furtherance of a legitimate law enforcement purpose;

Commentary to Standard 25-6.2(c)

There are legitimate law enforcement disclosures unrelated to active investigations, including officer training and the review of audit logs required by Standards 25-6.1(b)(i) and 25-7.1. Thus, this Standard permits disclosure for non-investigatory legitimate law enforcement purposes, so long as the record is appropriately redacted given the limited purpose of the disclosure.

Because the purposes are non-investigatory, the Standard cannot utilize the official certification of Standard 25-5.2(c). But it uses the same process to achieve accountability: requiring a written determination by a politically accountable law enforcement official. This is meant to be defined by reference to Standard 25-1.1(f), "politically accountable official," absent that Standard's reference to a civil equivalent. Thus, a "politically accountable law enforcement official" is "an upper-level law enforcement official . . . who is either elected or appointed by an elected official, or who is specifically designated for this purpose by an elected or appointed official."

(d) Disclosure of identification records of wanted or dangerous persons and stolen items upon the request of a law enforcement officer or prosecutor; and

Commentary to Standard 25-6.2(d)

Since its inception in 1967, local, state, and federal law enforcement agents have come to depend upon the FBI's National Crime Information Center ("NCIC"),[383] and officers should be able to submit queries to such databases in order ensure their safety and the effective enforcement of the criminal laws. NCIC contains information on wanted and missing persons; persons charged with serious offenses; individuals designated by the Secret Service as dangerous to the President; members of violent criminal gangs; members of terrorist organizations; unidentified persons; and stolen vehicles, license plates, boats, guns, securities, and other articles.[384]

(e) Other disclosures only if permitted by statute or upon a finding of a court that the public interest in such disclosure outweighs the privacy of the affected parties.

Commentary to Standard 25-6.2(e)

A jurisdiction might decide that certain records should be available to private organizations for purposes of licensing or employment, or even that the general benefits of open government favor open access even to private records obtained in criminal investigations (though presumably requiring those records to be redacted in certain respects). This Standard recognizes the efficacy of those decisions.

383. *See* http://www.fas.org/irp/agency/doj/fbi/is/ncic.htm (last visited July 2, 2012).

384. *See* Notice of Modified Systems of Records, 64 Fed. Reg. 52343 (Sept. 28, 1999).

Part VII. Accountability

Standard 25-7.1 Appropriate sanctions

The legislature should provide accountability for the provisions governing access to and storage and disclosure of records maintained by institutional third parties via appropriate criminal, civil, and/or evidentiary sanctions, and appropriate periodic review and public reporting.

Commentary to Standard 25-7.1

There were two constants in the drafting of these Standards as to accountability: a consensus that laws and regulations adopted according to these Standards should be meaningfully enforced via appropriate sanctions, and that the Standards would take no position on the suppression of evidence. Although at various stages the specifics of sanctions were discussed, ultimately the decision was to leave those specifics to legislatures. Thus, these Standards do not take any position on the specifics of administrative, civil, criminal and/or evidentiary sanctions, nor on the specifics of requiring periodic review and public reporting. Instead, they recognize that legislatures should provide meaningful accountability through some combination of these measures.

Despite this lack of black letter guidance, it might be helpful to note a few of the themes that developed during preliminary discussions. First, although ideally legislatures will carefully consider these Standards and adopt laws in conformity therewith, the Standards provide guidance even independent of legislative action, and likewise independent of court action. In significant part, and subject to existing laws and ordinances, they can be adopted by individual law enforcement agencies and prosecutorial offices. Either way, meaning whether such voluntary adoption takes place, or whether the Standards are imposed upon those agencies, decision makers might want to consider some form of mandatory administrative proceeding and/or sanction for material violations, in order to foster a culture of respect for the privacy these Standards are

meant to ensure. Potential administrative sanctions might include those requiring referral to an independent licensing body for attorneys or police. While a mandatory triggering provides some teeth, a trustworthy source should retain discretion over the magnitude of any sanctions in order to account for all relevant circumstances.[385]

Civil liability not only provides some redress for those harmed by a violation, but also incentivizes compliance. But while it is likely generally appropriate to permit civil liability against a government entity or institutional third party for negligent material violations, such liability is unlikely to be necessary to deter individual agents or employees of third parties, at least if administrative sanctions are available. There is a risk of over-deterring individual officers from vigorously pursuing those who would do social harm, and a risk of deterring individual employees from vigorously completing their employment responsibilities. A legislature might also want to consider providing qualified immunity to law enforcement agencies and institutional third parties that themselves provide adequate training, resources, discipline, and accountability regarding the laws implementing these Standards. The downside of qualified immunity is that there can be a violation and resulting harm without a remedy. However, that negative can be offset by the increased incentive to adhere to the relevant laws.

Criminal liability provides perhaps the ultimate incentive, and is sometimes used to ensure the privacy of records.[386] It is also a blunt instrument, however, and should be reserved for the worst offenses, meaning legislatures might consider criminalizing only certain willful violations, where "willful" designates a knowing violation of a known legal duty.

Just as periodic reviews of Privacy Act systems of records[387] and wiretaps[388] help law enforcement and legislators understand and better regulate those tools, periodic reviews of the records access within the ambit of these Standards will provide decision makers the data they require to ensure that the system is functioning effectively, both in terms of permitting law enforcement the information and resources it requires and in

385. *See, e.g.*, 18 U.S.C. § 2712(c) (triggering an administrative review for possibly willful or intentional violations).

386. *E.g.*, 5 U.S.C. § 552a(i)(1).

387. *See* 5 U.S.C. § 552(a)(s).

388. *See* 18 U.S.C. § 2519.

terms of respecting privacy. Audits also deter misuse, as those accessing records know in advance that their actions will be reviewed, and such audits can detect and prove any misuse that nonetheless occurs. Of course, resources dedicated to reviews, audits, and other compliance procedures are resources not available for investigating crime, and legislatures should be careful to account for such impositions.

Finally, public reporting can also foster accountability, and permits interested and knowledgeable parties to participate in discussions leading to improvements in the relevant laws and regulations. Where a legislature decides that periodic reviews, audits, and/or public reporting should be required, it should provide sufficient incentives to ensure reasonable compliance therewith.