Journal of Criminal Law and Criminology

Volume 103 | Issue 3 Article 5

Summer 2013

Real-Time and Historic Location Surveillance After United States v. Jones: An Administrable, Mildly Mosiac Approach

Stephen E. Henderson

0091-4169/13/10303-0803
THE JOURNAL OF CRIMINAL LAW & CRIMINOLOGY Vol. 103, No. 3

Printed in U.S.A.

REAL-TIME AND HISTORIC LOCATION SURVEILLANCE AFTER *UNITED STATES V. JONES*: AN ADMINISTRABLE, MILDLY MOSAIC APPROACH

STEPHEN E. HENDERSON*

In United States v. Jones*, the government took an extreme position: so far as the federal Constitution is concerned, law enforcement can surreptitiously electronically track the movements of any American over the course of an entire month without cause or restraint. According to the government, whether the surveillance is for good reason, invidious reason, or no reason, the Fourth Amendment is not implicated. Fortunately, the Supreme Court unanimously rejected that position. The Court did not, however, resolve what restriction or restraint the Fourth Amendment places upon location surveillance, reflecting proper judicial restraint in this nuanced and difficult area. Using the newly enacted American Bar Association (ABA) Standards on Law Enforcement Access to Third Party Records, this Article develops a regulatory regime for law enforcement visual surveillance, technologically enhanced location surveillance, and access to historic location records (e.g., cell site data). The proposal handles the administrative difficulties inherent in so-called mosaic approaches via a generally permissive regime regulated through an abuse standard. Ideally, such a proposal would be legislatively enacted with the backdrop of constitutional judicial review, and the Article comments upon*

* Professor of Law, The University of Oklahoma College of Law. Yale Law School (J.D., 1999); University of California at Davis (B.S., 1995). I am grateful to the *Journal of Criminal Law and Criminology*, and in particular to Symposium Editor Lily Katz, for the invitation to participate in the Symposium, and for the hospitality during that event. I continue to serve as Reporter for the American Bar Association Standards on Law Enforcement Access to Third Party Records, the blackletter to which has been adopted but the Commentary to which remains under development. Therefore, where I speak to the Commentary I do so with a well-informed, but nonetheless single, opinion. I am grateful to Jules Epstein, Susan Freiwald, Christopher Slobogin, and Andrew Taslitz for comments and critiques on an earlier version of this Article.

the need for constructive dialogue and initiative in that process by the law enforcement community, a view influenced by six years serving as Reporter for the ABA Standards.

TABLE OF CONTENTS

I. CELL TOWER DUMPS, LAW ENFORCEMENT, AND PRIVACY

The aim of this Article is to develop an administrable set of regulations for both historic and real-time law enforcement location surveillance. In order to do that, it is critical to understand how and why law enforcement might access such information. I therefore begin by describing a clever investigation and the relevance of *United States v. Jones*, and then turn to developing regulations.

A. THE HIGH COUNTRY BANDITS

Ronald Capito and Joel Glore, dubbed the "High Country Bandits," robbed sixteen banks in four states.[1] Their downfall was that they chose to carry and use a tracking device during and near those robberies. Although that sounds especially dumb, and it admittedly is not all that smart, most of us carry such a device, and many of us carry one at almost all times: a cellular phone. From among the victim banks, police selected several of the

[1] Larry Hendricks, *18 Years in Prison for High Country Bandit*, ARIZ. DAILY SUN (June 6, 2012, 9:00 AM), http://azdailysun.com/news/local/crime-and-courts/1b1634ee-8909-55de-bf87-8e3962e29eaf.html. The two robbed banks in Arizona, Colorado, Utah, and New Mexico. *See id.*; *see also* Larry Hendricks, *FBI: 'Bandits' Gambled Away Loot*, ARIZ. DAILY SUN (Mar. 13, 2010, 5:15 AM), http://azdailysun.com/news/local/crime-and-courts/fbi-bandits-gambled-away-loot/article_1d7d6c24-4090-531b-9f50-d9b3d002c57f.html.

more remote locations and gathered the phone records pertaining to the cell towers nearest those banks at the relevant times. Using a computer, they searched through the records, which pertained to 150,000 subscribers, and found two phones were used at every location. One belonged to Capito, and one belonged to Glore.[2]

This was not the first time that accessing all records pertaining to certain cell towers—known as "tower dumps"—has solved a string of bank robberies,[3] and it is plainly good police work. Indeed, a similar basic modus operandi appears to have been used in the investigation that resulted in the resignation of CIA Director David Petraeus.[4] Such records access is thus good police work, but it is also invasive of privacy. In the Petraeus investigation, which reads like a soap opera, it is very easy to see the personal ramifications.[5] In the investigation of the High Country Bandits, the phone records of 150,000 persons were perused. Moreover, a cell phone is in regular communication with the nearest cell tower anytime it is

---

[2] Eric Betz, *Bank 'Bandit' Pleads Guilty*, ARIZ. DAILY SUN (Nov. 8, 2011, 9:00 AM), http://azdailysun.com/news/local/crime-and-courts/bank-bandit-pleads-guilty/article_90aee950-0b4c-59da-ac56-7a5869d1cab4.html.

[3] The first use appears to be the apprehension of the so-called Scarecrow Bandits in 2008. *See* Press Release, U.S. Attorney's Office for the N. Dist. of Tex., Federal Jury Convicts Scarecrow Bandits on Bank Robbery and Firearm Offenses (Aug. 13, 2009), *available at* http://www.justice.gov/usao/txn/PressRel09/scarecrow_bandits_convict_pr.html. "The defendants were known as the Scarecrow Bandits by the FBI because they wore loose, sometimes plaid, shirts and floppy hats during the first several of the 21 robberies they are believed to have committed." *Id.* They turned to more paramilitary tactics in later robberies. *See id.*; *see also* Government's Response to Supplemental Motion to Suppress Wiretap at 2, United States v. Hewitt, No. 3:08-CR-167-B (N.D. Tex. June 26, 2009) ("[T]he FBI obtained cell site 'dump' records for a dozen banks robbed by the Scarecrow Bandits . . . . A 'dump' record reflects all of the cellular telephones that were using the cell tower closest to the given bank at the time it was robbed . . . ."); Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 119–20 (2012) (describing this investigation and another using cell tower dumps).

[4] FBI agents began with anonymous e-mails we now know to have been sent by Petraeus's jealous mistress and biographer, Paula Broadwell. *See* Michael Isikoff & Bob Sullivan, *Emails on 'Coming and Goings' of Petraeus, Other Military Officials Escalated FBI Concerns*, NBC NEWS (Nov. 12, 2012, 8:30 PM), http://openchannel.nbcnews.com/_news/2012/11/12/15119872-emails-on-coming-and-goings-of-petraeus-other-military-officials-escalated-fbi-concerns?lite. If, say, Broadwell had signed up for a Yahoo! e-mail account using bogus personal information while using a hotel's Internet service, the e-mail could be traced back to that hotel via the Internet protocol address of that service. By coordinating the locations from which multiple e-mails were sent with the guest lists at those hotels or other providers, agents were able to track them to Broadwell—indeed, the locations coincided with travel promoting her Petraeus biography, ironically titled *All In*. *See id.*; *see also* PAULA BROADWELL, ALL IN: THE EDUCATION OF GENERAL DAVID PETRAEUS (2012).

[5] *See* Scott Shane, *Petraeus Case: Issue of Privacy Is in Play, Too*, N.Y. TIMES, Nov. 14, 2012, at A1.

"active," meaning anytime it is turned on.[6] Were this not the case, it would be impossible to receive a telephone call. And while providers today typically only store location information when a call is in progress, they are likely to begin more broadly storing the location of a phone anytime it is active.[7] Thus, cellular phone providers will potentially possess a virtually complete record of a customer's location at all times, and that vast record can be mined by police.[8]

The reasonable question, therefore, is what restraints or regulations the law should place upon such access. In the investigation of the High Country Bandits, a court order was used to obtain the cellular records, and police selected the most rural bank locations "in order to minimize the amount of extraneous telephone data that would likely be obtained."[9] Once police searched those records and located two phone numbers of interest, they proceeded to obtain further record information.

For the first telephone number, police could have subpoenaed the subscriber's identifying information from the telephone provider.[10] But because they also wanted to acquire further transactional records pertaining to the phone, they probably used a single "specific and articulable facts" court order.[11] They learned that this phone was registered to Capito.[12] The second number was assigned to a prepaid phone, meaning the subscriber was not required to provide identifying information or, at least, accurate identifying information. Fortunately for police, Glore was accommodating and upon purchase had provided his name and date of birth.[13] The acquired

---

[6] *See ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary* [hereinafter *Location Based Technologies Hearing*], 111th Cong. 12–14 (2010) (testimony of Professor Matt Blaze).

[7] *See id.* at 16, 27, 95. The accuracy of that location will also continue to increase. *See id.* at 15, 20, 26–27, 30, 95; *see also Finding the Way Inside*, ECONOMIST, Dec. 1, 2012, at 18 (describing new mobile phone technologies that, unlike GPS, enable tracking location *within* buildings).

[8] A historic record also permits accurate prediction. One study using mobile phone data found that location is 93% predictable. Chaoming Song et al., *Limits of Predictability in Human Mobility*, 327 SCIENCE 1018, 1020 (2010), *available at* http://www.barabasilab.com/pubs/CCNR-ALB_Publications/201002-19_Science-Predictability/201002-19_Science-Predictability.pdf; *see also Dr. Seldon, I Presume*, ECONOMIST, Feb. 23, 2013, at 76. In the words of the study, "a historical record of the daily mobility pattern of the users hides an unexpectedly high degree of potential predictability." Song, *supra*, at 1020.

[9] Criminal Complaint at 13, United States v. Capito, No. 3:10-CR-08050-NVW (D. Ariz. Mar. 12, 2010).

[10] *See id.* at 14–15 (identifying the phone number and provider); *see also* 18 U.S.C. § 2703(c)(2) (2006).

[11] *See* 18 U.S.C. § 2703(c)(1)(B), (d).

[12] *See* Criminal Complaint, *supra* note 9, at 15.

[13] *Id.*

call detail records for both phones—noting when calls were placed or received and at what geographic location—corroborated the police's suspicion.[14]

Police conducted physical searches and further records searches.[15] As for records, police used Google and Internet databases of property records, and obtained records held by the commercial data aggregator and broker ChoicePoint,[16] a motor vehicle department, courts, casinos, hotels, and a gas station.[17] From this single investigation it is evident that records access is vitally important to effective law enforcement, and extremely commonplace. Records access can solve a murder, as when police caught a serial killer by tracing a map he generated online.[18] And records access can defuse an emergency, as when police tracked the location of a cell phone from which a sister had received a chilling message: "The girl with this phone is dead . . . ."[19]

Once again, the reasonable question is therefore what restraints or regulations should be placed upon law enforcement records access. Perhaps some people believe that law enforcement access should not be regulated: we should entirely trust our privacy to the integrity of police officers.

---

[14] *See id.* at 15–16. The two phones "were either in very close proximity to each of the . . . sixteen bank robberies on the date and near the time of each robbery or the telephones can be documented traveling between the general area of [the suspects' hometown] to or from the general area of each bank during the respective time frame of each robbery." *Id.* at 16.

[15] Searches of Capito's and Glore's residences and vehicles located significant incriminating information, and while Capito "lawyered up," Gore confessed. *See id.* at 28–31.

[16] ChoicePoint was subsequently purchased by LexisNexis. *See Acquisition of ChoicePoint Inc. Completed*, REED ELSEVIER, http://www.reedelsevier.com/mediacentre/pressreleases/2008/Pages/AcquisitionofChoicePointIncCompleted.aspx (last visited Apr. 10, 2013); *Risk Solutions*, LEXISNEXIS, http://www.lexisnexis.com/risk/ (last visited Mar. 18, 2013).

[17] *See* Criminal Complaint, *supra* note 9, at 20–25.

[18] *See* Stephanie Simon, *Virtual Trail Led to Serial Killer Suspect*, L.A. TIMES, June 17, 2002, at A8.

> [I]n response to a federal subpoena, Expedia.com was able to pull up the IP address of every user who had looked at a West Alton map in recent days. As it turned out, there was only one: IP 65.227.106.78. The user assigned to that number had clicked to zoom in on West Alton 10 times—until the map on his screen looked exactly like the version sent to the [newspaper].

Id.; *see also* Tim O'Neil, *Police Tie Man to at Least 12 Killings*, ST. LOUIS POST-DISPATCH, June 25, 2002, at B1.

[19] *See* Rocco Parascandola & Sarah Armaghan, *Queens Woman Who Vanished Sunday Found Alive and Well in Texas*, N.Y. DAILY NEWS (July 12, 2012, 8:58 PM), http://www.nydailynews.com/new-york/queens-woman-vanished-sunday-found-alive-texas-article-1.1113459. Fortunately, it seems the missing sister ran away to escape plans for an arranged marriage, rather than suffered a violent demise. *See id.*

Perhaps some people believe that law enforcement access should be *highly* regulated: we should place a neutral and detached magistrate between citizens and the officer engaged in the "competitive enterprise of ferreting out crime,"[20] and that magistrate should make a demanding substantive inquiry before permitting access. Perhaps some people believe that law enforcement access should be *constitutionally* regulated, meaning the source of this regulation should be the federal and/or state constitution. Perhaps some people believe the source should be statutory. When one considers the diversity of records information, *reasonable* people, I submit, believe there should be some constitutional regulation, some statutory regulation, and some things left to officer integrity. The details of specific regulations applying to particular types of information will be contested and difficult. But those details are worth working out because the binary alternatives—either zero regulation or "total" regulation—are completely unacceptable. We require legislative differential regulation, by which I mean a hierarchy of regulation proportional to privacy, yet responsive to law enforcement needs, subject to a constitutional backstop.

B. THE RELEVANCE OF *UNITED STATES V. JONES*

This need for regulation is why *United States v. Jones*[21] was a unanimous decision as to the prevailing party. The government took an egregious position, namely that law enforcement can surreptitiously electronically track the movements of any American over the course of an entire month without any Fourth Amendment restraint.[22] In this instance the tracking was via a GPS device attached to the defendant's vehicle, but as I have described, that same information could be obtained from third-party records. And it was not difficult for the Justices to recognize that such tracking could be used against them. At oral argument, Justice Roberts asked just that.[23] Now that technology has removed the formerly significant resource restraints on tracking location, it is possible to track all of us. But it was more than self-interest that generated a nine-to-zero loss for the government. It was the common sense that in a free and democratic society, and one in which at least some law enforcement abuse has been known to occur,[24] law enforcement should not be permitted to engage in

---

[20] Johnson v. United States, 333 U.S. 10, 14 (1948).

[21] 132 S. Ct. 945 (2012).

[22] *Id.* at 951.

[23] *See* Transcript of Oral Argument at 9–10, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259), *available at* http://www.supremecourt.gov/oral_arguments/argument_transcripts/10-1259.pdf.

[24] *See, e.g.*, DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 180, 183–85 (2004); Editorial, *Backward at the F.B.I.: Overreaching*

such long-term tracking without restraint.

What restraint did the Justices select, at least as to the GPS tracking before the Court? Not a single Justice answered this question. Justice Scalia, writing for a majority of five, focused on the installation of the GPS device and held that a trespass to a constitutionally protected person, house, paper, or effect in order to obtain information constitutes a Fourth Amendment search, thus resurrecting the pre-*Katz* trespass- or property-based Fourth Amendment.[25] But the Court did not decide whether a warrant or some other judicial preclearance was necessary, or what quantum of suspicion was required for that search to be reasonable.[26] Justice Alito, writing for a concurring four, instead held that the long-term electronic monitoring of location constitutes a search because it invades a reasonable expectation of privacy.[27] And Justice Sotomayor, who joined the majority, also wrote a separate concurrence agreeing with Alito.[28] So we have two conceptions of Fourth Amendment search, both of which were satisfied, but no answer as to what law enforcement must know or do before conducting that search.[29]

This lack of guidance is not surprising, not only because the government had not argued the issue—thinking nothing necessary to justify its actions—but also because that guidance is difficult. Two terms before, the Court punted when it came to the Fourth Amendment regulation of another type of record—text messages in the hands of a service provider.[30] And in *Jones*, Alito stressed what Professor Daniel Solove and others have argued, which is that it would be ideal for legislatures to take a first stab at

---

New Rules for Surveillance Threaten Americans' Basic Rights, N.Y. TIMES, June 19, 2011, at WK7; *F.B.I. Obtained Reporters' Phone Records*, N.Y. TIMES, Aug. 9, 2008, at A15; Mark Mazzetti & Eric Lichtblau, *Pentagon Review Faults Demands for Bank Records*, N.Y. TIMES, Oct. 14, 2007, at A28; John O'Neil, *F.B.I. Director Is Bombarded by Stinging Questions at Senate Hearing*, N.Y. TIMES, May 3, 2006, at A23; Julian Sanchez, *Wiretapping's True Danger*, L.A. TIMES, Mar. 16, 2008, at M9; Charlie Savage, *F.B.I. Violated Rules in Obtaining Phone Records, Report Says*, N.Y. TIMES, Jan. 21, 2010, at A25; Frederick A. O. Schwarz, Jr., Letter to the Editor, *Rights Abuses by the F.B.I.: A Look at the History*, N.Y. TIMES, Oct. 5, 2010, at A30; Scott Shane, *Senators Cite F.B.I. Failures as Chief Promises Change*, N.Y. TIMES, Mar. 28, 2007, at A16.

[25] *See Jones*, 132 S. Ct. at 950–52. For further description of the Court's opinions, see Stephen E. Henderson, *After* United States v. Jones*, After the Fourth Amendment Third Party Doctrine*, 14 N.C. J.L. & TECH. (forthcoming 2013).

[26] *See Jones*, 132 S. Ct. at 954.

[27] *See id.* at 962–64 (Alito, J., concurring in the judgment).

[28] *See id.* at 954–56 (Sotomayor, J., concurring).

[29] *See* State v. Brereton, 826 N.W.2d 369, 381 (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).

[30] *See* City of Ontario v. Quon, 130 S. Ct. 2619, 2629–30 (2010) (assuming a reasonable expectation of privacy).

these complicated questions, after which courts can review whether those solutions meet the constitutional floor.[31]

I can personally attest to the difficulty of articulating guidance. For the past six years, I have served as Reporter for a new set of ABA Criminal Justice Standards, entitled Law Enforcement Access to Third Party Records (LEATPR). The ABA process is appropriately thorough and rigorous, consisting of several stages at which all interested parties have a voice.[32] In February 2012, the ABA House of Delegates approved consensus blackletter standards.[33]

The remainder of this Article is structured as follows: First, the initial portions of Part II consider how the ABA LEATPR Standards treat law enforcement access to location information, and more generally how legislatures and courts should regulate such access (Parts II.A and II.B). Given that law enforcement requested some information from cell phone providers over 1.3 million times in 2011,[34] and given *Jones*, consideration of this specific type of record is especially timely. I conclude that absent consent or an emergency, the following would be reasonable: law enforcement would need a warrant to access over twenty-four hours of location information, could access a lesser period of location information using a lesser court order, and could access a record indicating location at a single point in time for any legitimate law enforcement purpose. Part II.C briefly considers some lingering issues regarding the probable cause required to obtain a location warrant, after which Part II.D considers the difficulties inherent in any "mosaic" approach that differentiates access regulation by amount. I resolve these difficulties by typically not requiring police to consider past requests, but punishing abuse of the lesser process. Applying this structure to the investigation of the High Country Bandits implicates another powerful aspect of the LEATPR Standards (Part II.E), and Part II.F therefore explains and applies the Standards' incorporation of

---

[31] *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment); Daniel J. Solove, Essay, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1515, 1535–37 (2010).

[32] *See* Martin Marcus, *The Making of the ABA Criminal Justice Standards: Forty Years of Excellence*, 23 CRIM. JUST. 10 (2009), *available at* http://www.americanbar.org/content/dam/aba/publications/criminal_justice_magazine/makingofstandards_marcus.authcheckdam.pdf.

[33] *See* CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS (2012), *available at* http://www.americanbar.org/content/dam/aba/publications/criminal_justice_standards/Black_Letter.authcheckdam.pdf.

[34] *See* Eric Lichtblau, *More Demands on Cell Carriers in Surveillance*, N.Y. TIMES, July 9, 2012, at A1; Press Release, Congressman Ed Markey, Markey: Law Enforcement Collecting Information on Millions of Americans from Mobile Phone Carriers (July 9, 2012), *available at* http://markey.house.gov/press-release/markey-law-enforcement-collecting-information-millions-americans-mobile-phone-carriers.

de-identification. Part III then considers real-time location surveillance, which is outside the scope of the Standards but nonetheless influenced by their guidance. I propose regulation that is analogous to that for records access except that it must acknowledge the realities of police patrols. Finally, Part IV comments on the importance of forthright and open dialogue to the process of regulating law enforcement access.

II. LOCATION RECORDS UNDER THE ABA LEATPR STANDARDS

In February 2012, the ABA House of Delegates approved a twenty-fifth volume in its Criminal Justice Standards entitled Law Enforcement Access to Third Party Records.[35] A background Report to the Standards was submitted to the House of Delegates and is currently available,[36] and very extensive commentary is being drafted. Because the interested reader can turn to those sources, I will provide only a brief summary.

A. OVERVIEW OF THE STANDARDS

The Standards consist of seven Parts: I. Definitions; II. Scope; III. General Principles; IV. Categorization of Information and Protection; V. Access to Records; VI. Retention, Maintenance, and Disclosure of Records; and VII. Accountability. The four principles of Part III nicely summarize the "why" and the "what" of the Standards. In essence, (1) modern third parties maintain easily searchable records containing vast amounts of personal information,[37] (2) access to those records can be essential to law enforcement functions,[38] (3) such law enforcement access

---

[35] CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS (2012).

[36] AM. BAR ASS'N, BACKGROUND REPORT TO CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS (2012), *available at* http://www.americanbar.org/content/dam/aba/publications/criminal_justice_standards/Memo_House.authcheckdam.pdf.

[37] Standard 25-3.1 provides:

> 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.

CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS § 25-3.1.

[38] Standard 25-3.2 provides:

> 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.

can infringe privacy and chill fundamental freedoms,[39] and therefore (4) decisionmakers should carefully consider how best to regulate that access.[40]

Hence, the Standards "relate to law enforcement investigatory access to, and storage and disclosure of, records maintained by institutional third parties."[41] Location information residing with a cell phone service provider is thus squarely within the Standards, as an institutional third party is defined to include "any nongovernmental entity."[42]

The Standards do not suggest a particular regulation for given types of information. Although, everything else being equal, more specific guidance is always better, over the six years of work it became clear not only that there are a range of reasonable opinions when it comes to this ultimate question, but also that those opinions will vary by local experience and need, and that both the law and technology are very much in a state of flux. Therefore, as noted in Standard 3.4, the Standards provide a framework, or algorithm, via which the appropriate decisionmaker—for example, a legislature—can determine precisely what regulation to place upon a particular type of law enforcement access. Before the passage of the Standards, there was no framework for making these determinations. While there is significant collective wisdom in the many existing statutes, court opinions, and administrative rules regulating law enforcement access to record information, it is scattered, causing rules to at times be ad hoc, confusing, and inconsistent.[43] The Standards' framework thus provides

---

Id. § 25-3.2.

[39] Standard 25-3.3 provides:

> 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.

Id. § 25-3.3.

[40] Standard 25-3.4 provides:

> 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.

Id. § 25-3.4.

[41] *Id.* § 25-2.1.

[42] *Id.* § 25-1.1(e). "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." *Id.* § 25-1.1(g).

[43] For example, we have relatively strong protection for video rental records because the rental habits of Judge Bork happened to become an issue during his confirmation hearings. *See* Somini Sengupta, *Hulu Faces a Privacy Test in Federal Court*, N.Y. TIMES, Aug. 20, 2012, at B4; Natasha Singer, *Put It on My Marquee: I Just Watched 'Creepshow 2,'* N.Y. Times, Dec. 11, 2011, at BU3; Natasha Singer, *Technology Outpaces Privacy (Yet Again)*,

much needed guidance to those confronting these complex problems.

Although application will at times be unavoidably difficult, the Standards' operation is straightforward. A decisionmaker first considers the privacy level of a given type of information, in this case location information. This requires considering a few things. Why is this information in the hands of the third party?[44] Is that transfer something we need to be wary of chilling? How personal is the information?[45] Will its access tend to be embarrassing or stigmatizing? Is the information being accessed by others?[46] Does existing law speak to the access of this or similar information?[47] Together these considerations dictate how private is a type of information. For example, where on the spectrum of privacy does location information fall? Is location information highly private, moderately private, minimally private, or not private? In other words, are we talking large, medium, small, or nothing at all?[48]

That privacy sets a threshold for law enforcement access, just as the privacy of a home sets the Fourth Amendment standard for entering at a warrant supported by probable cause. When there is no emergency, the nonconsensual entry into a home requires a warrant.[49] And other than on the extreme margins, the Fourth Amendment does not differentiate between "serious" and "petty" crimes with respect to this warrant requirement.[50] Nor does the law ease the warrant requirement when crime rates go up or

---

N.Y. TIMES, Dec. 12, 2010, at BU3. And we seemingly have more significant regulation for historic access to communication transactional information than for real-time access. *See* 18 U.S.C. § 2703(c)(1)(B), (d) (2006) (requiring a "specific and articulable facts" court order for historic records); *id.* § 3123(a)(1) (requiring prosecutor certification of relevance for real-time access).

[44] *See* CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS § 25-4.1(a).

[45] *See id.* § 25-4.1(b).

[46] *See id.* § 24-4.1(c).

[47] *See id.* § 24-4.1(d).

[48] Why four categories, and not three or five? As Anthony Amsterdam cogently observed many years ago, there is no perfect number because "any number of categories, however shaped, is too few to encompass life and too many to organize it manageably." Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 377 (1974). There is an unavoidable tradeoff between nuance and administrability.

[49] *See* Payton v. New York, 445 U.S. 573, 586 (1980).

[50] *See* Welsh v. Wisconsin, 466 U.S. 740, 754 (1984) (prohibiting warrantless entry for a nonjailable traffic offense); Illinois v. McArthur, 531 U.S. 326, 335–36 (2001) (distinguishing *Welsh* for a jailable narcotics offense); Atwater v. City of Lago Vista, 532 U.S. 318, 348–49 (2001) (questioning more generally the administrability of such distinctions and therefore rejecting a differential Fourth Amendment based upon them as to warrantless arrests in public). For a general discussion of the pitfalls in considering magnitude of crime under the Fourth Amendment, see Christopher Slobogin, *Why Crime Severity Analysis Is Not Reasonable*, 97 IOWA L. REV. BULL. 1 (2012).

when a novel crime is first practiced. Hence, under the Standards, records containing highly private information default to being highly protected, records containing moderately private information default to being moderately protected, and records containing minimally private information default to being minimally protected.[51] Absent consent[52] or an emergency,[53] accessing records containing highly protected information requires a probing judicial authorization (a judicial determination of probable cause),[54] accessing records containing moderately protected information requires a lesser judicial authorization,[55] accessing records containing minimally protected information requires a prosecutorial or administrative subpoena,[56] and accessing unprotected records is permissible upon officer request for any legitimate law enforcement purpose.[57]

However, these threshold regulations are subject to a caveat. Law enforcement is understandably concerned that restricting access to certain records could make it markedly more difficult to perform its essential functions. And while accessing third-party records has very real implications for privacy, and privacy has very real implications for our fundamental rights, accessing records does not have the immediate danger to life and limb present in physical searches of suspects or their property. Thus, there is a safety valve:

> If the [default] limitation . . . 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.[58]

It is critical that these two decisions—how private the information is and then how protected it should be—are kept separate and sequential. If they are conflated, the more amorphous but equally important privacy

---

[51] *See* CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS § 24-4.2.

[52] *See id.* § 25-5.1.

[53] *See id.* § 25-5.4.

[54] *See id.* § 25-5.3(a)(i). The Standards also acknowledge the historically favored role of a grand jury subpoena, even though this is substantively questionable given the effectively total prosecutorial discretion. Standard 25-2.1(c) carves from the Standards' scope "access to records via a grand jury subpoena, or in jurisdictions where grand juries are typically not used, a functionally equivalent prosecutorial subpoena."

[55] *See id.* § 25-5.3(a)(ii). This Standard recognizes a judicial determination of reasonable suspicion, a judicial determination of relevance, and a prosecutorial certification of relevance. *See id.* § 25-5.2(a)(ii)–(iv).

[56] *See id.* § 25-5.3(a)(iii).

[57] *See id.* § 25-5.3(d).

[58] *Id.* § 25-4.2(b).

interests are almost surely to be unfairly discounted.

There is much more to the Standards, some of which will be considered below, but this explains their general structure. A decisionmaker engages in a three-step process: (1) How private is this type of information? (2) What restriction should that dictate? (3) Despite the general wisdom of those first two steps, would that restriction on accessing this particular type of record information be more harmful than beneficial?

B. APPLICATION TO LOCATION INFORMATION

Armed with a general understanding of the LEATPR Standards, we can turn to the specific inquiry of interest: what should be the restriction on law enforcement access to location records residing with cell phone providers? We know a decisionmaker must determine how private such information is, which requires analyzing the factors described above. And "[i]n making that determination, a legislature, court, or administrative agency should consider present and developing technology."[59] Technology has progressed such that these records can pinpoint location very accurately, and that accuracy will continue to increase as, among other changes, more cell towers are added to provider networks.[60]

The first privacy factor is the extent to which "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."[61] While I will leave a full discussion of these factors to the much more expansive Standards Commentary, this factor recognizes that sharing is relevant to privacy, but also that information privacy—which is fundamentally about control—is divisible and is not limited to secrecy.[62] Moreover, where a transfer is conducive to other values, especially constitutionally enshrined ones like the freedom of speech and association, the law should be wary of chilling that transfer. In the words of Justice Sotomayor, "Awareness that the government may be watching chills associational and expressive freedoms."[63]

In order to use a mobile telephone, a customer must communicate his or her location to the service provider; without this information, the

---

[59] *Id.* § 25-4.1.

[60] *See Location Based Technologies Hearing*, *supra* note 6, at 15, 20, 26–27, 30, 95 (testimony of Matt Blaze).

[61] CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS § 25-4.1(a).

[62] *See* Stephen E. Henderson, *Expectations of Privacy in Social Media*, 31 MISS. C. L. REV. 227, 232–33 (2012).

[63] United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

provider would be unable to send and receive calls. Mobile telephony contributes to the freedoms of expression and association, but for many years its contribution arguably 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 has changed.[64] Not only do 87% of American adults own a mobile phone,[65] but 46% are users of the more sophisticated smartphones.[66] Protestors use their mobile phones to communicate with interested parties,[67] and concerned citizens use them to record possible police abuse.[68] People increasingly use their phones to obtain navigation directions and to locate nearby businesses or other locations of interest.[69] In refusing to decide the Fourth Amendment status of what are now essentially obsolete 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."[70]

The second privacy factor is the extent to which "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."[71] Limited location information is routinely provided to countless passersby, is stored in innumerable records

---

[64] There are over 285 million active wireless subscriber accounts in the United States. *See In re* Application of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 834 (S.D. Tex. 2010). By 2010, they accounted for over 2.2 trillion minutes of use and 1.56 trillion text messages. *Id.* at 835.

[65] *Trend Data (Adults)*, PEW INTERNET & AM. LIFE PROJECT, http://pewinternet.org/Trend-Data-%28Adults%29/Device-Ownership.aspx (last visited Mar. 27, 2013) (citing statistics as of December 2012).

[66] Aaron Smith, *Nearly Half of American Adults Are Smartphone Owners*, PEW INTERNET & AM. LIFE PROJECT (Mar. 1, 2012), http://pewinternet.org/Reports/2012/Smartphone-Update-2012.aspx.

[67] *See* Russ Buettner, *Judge Orders Twitter to Turn Over Protester's Messages*, N.Y. TIMES, July 3, 2012, at A17; Jennifer Preston, *Protesters Look for Ways to Feed the Web*, N.Y. TIMES, Nov. 25, 2011, at A28.

[68] *See* Eunice Lee, *Watching the Watchmen: ACLU Offers Citizens 'Stealth' App to Record Cops*, STAR-LEDGER (Newark, N.J.), July 3, 2012, at 1, 7; *The App Place: Police Tape*, AM. C.L. UNION OF N.J., http://www.aclu-nj.org/yourrights/the-app-place/ (last visited Mar. 18, 2013).

[69] *See* John R. Quain, *Getting Lost with a Cellphone*, N.Y. TIMES, Sept. 20, 2009, at A10.

[70] City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010).

[71] CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS § 25-4.1(b) (2012).

(e.g., a store receipt), and tells relatively little about a person. 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."[72] In the words of the New York Court of Appeals in the context of law enforcement location tracking:

> The 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.[73]

The third privacy factor is the extent to which "such information is accessible to and accessed by non-government persons outside the institutional third party."[74] This factor will very often be neutral. One of the reasons we consider information personal (the preceding privacy factor) is because we know it is not routinely accessed, and where it is routinely accessed, it is typically not considered personal. But there may be instances in which the type of information is personal—it is intimate and social norms typically keep such information within one's social network—but nonetheless certain such information is not only accessible to, but is routinely accessed by, persons having no authorization from the person to whom the information relates.[75] In that case, law enforcement need not alone shield its eyes. With respect to cell phone location information, I am not aware of any such relevant access.

The fourth and final privacy factor is the extent to which "existing law, including the law of privilege, restricts or allows access to and dissemination of such information or of comparable information."[76] Although it is the raison d'être of the Standards that decisionmakers should judiciously reconsider existing rules under the Standards' framework, it would be foolhardy to do so without regard to what has come before.

---

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

[73] People v. Weaver, 909 N.E.2d 1195, 1199–1200 (N.Y. 2009).

[74] CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS § 25-4.1(c).

[75] An example might be salaries for those working at a public institution.

[76] CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS § 25-4.1(d).

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

The federal constitutional law regarding law enforcement access to location information is currently in flux. From *United States v. Jones* we know that installing a GPS device on a vehicle is a Fourth Amendment search,[77] and that five Justices also believe that thereby obtaining long-term location information constitutes a Fourth Amendment search.[78] But while the privacy intrusion is identical, the Court has not yet had occasion to address to what extent its reasoning applies to accessing location information in the form of third-party records; only Justice Sotomayor spoke to records access in *Jones*.[79] Thus, we can expect to see disagreement among the lower courts.[80] Several state constitutions require a warrant for law enforcement location tracking,[81] but we once again lack opinions on historic access.

The federal statutory law regarding law enforcement access to third-party location information is a mess, both as to prospective access and historic access. One must interpret several complicated statutes that were written without an understanding of this modern technology.[82] The Third

---

[77] 132 S. Ct. 945, 949–53 (2012).

[78] *Id.* at 957–64 (Alito, J., concurring in the judgment); *id.* at 955–56 (Sotomayor, J., concurring); *cf.* United States v. Skinner, 690 F.3d 772, 777–81 (6th Cir. 2012) (holding that there is no Fourth Amendment restraint on law enforcement tracking a mobile phone in real time over several days).

[79] *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring). On remand the government has sought to rely upon cell site location information, so the *Jones* case may yet answer that question. *See* Mike Scarcella, *DOJ: No Privacy Rights in Cell Phone Tower Data*, BLOG OF LEGAL TIMES (Sept. 5, 2012, 3:23 PM), http://legaltimes.typepad.com/blt/2012/09/doj-no-privacy-rights-in-cell-phone-tower-data-.html. To date, however, the district court has avoided the question by relying upon the good-faith exception. *See* United States v. Jones, No. 05-0386 (ESH), 2012 WL 6443136, at *2, *17–19 (D.D.C. Dec. 14, 2012).

[80] *See, e.g.*, United States v. Graham, 846 F. Supp. 2d 384, 389 (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 the United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 846 (S.D. Tex. 2010) (disagreeing) (currently on appeal before the Fifth Circuit).

[81] People v. Weaver, 909 N.E.2d 1195, 1201–02 (N.Y. 2009); State v. Campbell, 759 P.2d 1040, 1049 (Or. 1988); State v. Jackson, 76 P.3d 217, 224 (Wash. 2003).

[82] 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* COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, U.S. DEP'T OF JUSTICE, 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 historic access, DOJ relies solely upon the noncontent provisions of the Stored Communications Act, again with mixed success. *See id.* at 122; *infra* notes 83–85.

Circuit, for example, has held that the statutes permit a magistrate to choose whether to require a warrant for access to historic cell site location information,[83] while other courts disagree,[84] and the issue is currently before the Fifth Circuit.[85] There are federal restrictions on a mobile phone provider choosing to disclose location information.[86] And we can expect to see more legislation in the near future. Bills introduced in several states and in Congress would restrict law enforcement access,[87] and the California legislature overwhelmingly supported a bill that would typically require a warrant to obtain historic location information, but the Governor vetoed it.[88]

Given (1) that location information must necessarily be provided in order to use a mobile phone, (2) that mobile phones are becoming increasingly pervasive in the discourses of society, (3) that individually location information is often shared but collectively location information is highly personal and almost never shared outside of the necessary transfer to the provider, (4) that such information is not accessed by others, and (5) that—while far too confusing—existing legal protections are significant, I could imagine a decisionmaker deciding the following: Location at a single point in time is not private, a relatively short period of location information (say up to twenty-four hours) is moderately private, and anything longer is highly private. This is of course not the only solution, but it strikes me as a reasonable one. As for a single datum of location information, the

---

[83] *See In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 319 (3d Cir. 2010). For a thorough explanation of the issues in this case and location tracking more generally, see Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681 (2011).

[84] *See In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 600 n.42 (W.D. Pa. 2008) (collecting cases).

[85] *See In re* Application of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827 (S.D. Tex. 2010); Jeffrey Brown, *Fifth Circuit to Hear Cell Site Data Case Tuesday*, CYBERCRIME REVIEW (Oct. 1, 2012), http://www.cybercrimereview.com/2012/10/fifth-circuit-to-hear-cell-site-data.html.

[86] *See* 47 U.S.C. § 222(f) (2006). For relevant legislative history and analysis, see *In re Application of the United States for Historical Cell Site Data*, 747 F. Supp. 2d at 841–43.

[87] *See* Somini Sengupta, *Courts Divided over Searches of Cellphones: Privacy Act Reviewed*, N.Y. TIMES, Nov. 26, 2012, at A1.

[88] *See* S.B. 1434, 2011–2012 Leg., Reg. Sess. (Cal. 2012); James Temple, *Brown Vetoes Bill on Location Privacy*, S.F. CHRON., Oct. 4, 2012, at D3. The Assembly approved the bill by a vote of 63–11 and the Senate by a vote of 33–3. *See Complete Bill History, Bill Number: S.B. No. 1434*, OFFICIAL CAL. LEGIS. INFO., http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_1401-1450/sb_1434_bill_20120930_history.html (last visited May 27, 2013); *see also SB 1434*, AROUND THE CAPITOL, http://www.aroundthecapitol.com/Bills/SB_1434/20112012/ (last visited Apr. 13, 2013). Similar legislation has been introduced in Congress. *See* H.R. 6529, 112th Cong. (2012).

potentially many people who observe a person know that person's location, and many records, including any store receipt, contain that information. On the other hand, presence at certain locations can be very personal, and we often do not take notice of the others present, and if we do, we typically quickly forget. So I could understand a categorization of either minimally private or not private, but for sake of argument I will choose not private.[89]

If so, the threshold protection would be that a single datum of location information is not protected, a day or less of location information is moderately protected, and more than a day of location information is highly protected. An invocation of the Standards' "safety valve," by which highly private information could be given lower protection,[90] would depend upon a demonstrated law enforcement need, a topic to which I will return shortly. Absent that lowering, and absent consent,[91] emergency aid,[92] and exigent circumstances,[93] law enforcement access to more than a day of location information would require "a judicial determination that there is probable cause to believe the information in the record contains or will lead to evidence of crime."[94] Law enforcement access to a day or less of location information would require one of three options: (1) "a judicial determination that there is reasonable suspicion to believe the information in the record contains or will lead to evidence of crime,"[95] (2) "a judicial determination that the record is relevant to an investigation,"[96] or (3) "a prosecutorial certification that the record is relevant to an investigation."[97] In other words, it would be entirely consistent with the Standards for a

---

[89] If a decisionmaker were to consider location at a single point in time to be minimally private, the Standard 25-4.2(b) escape valve might be used to lessen the protection. While there might be good reason to independently regulate access to certain types of store receipts, without a decrease in protection, access to *all* store receipts would be regulated, which might be a significant impediment to initial law enforcement investigation.

[90] *See* CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS § 25-4.2(b) (2012); *supra* note 58 and accompanying text.

[91] *See* CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS § 25-5.1.

[92] *See id.* § 25-5.4. "'Emergency aid' is government conduct intended to eliminate or mitigate what is reasonably believed to be imminent danger of death or serious physical injury." *Id.* § 25-1.1(a).

[93] *See id.* § 25-5.4. "'Exigent circumstances' are circumstances in which there is probable cause to fear imminent destruction of evidence or imminent flight." *Id.* § 25-1.1(b).

[94] *Id.* § 25-5.2(a)(i). A decisionmaker can decide to impose even greater restrains upon access to highly protected information, but that is expected to be rare in the records context. *See id.* § 25-5.3(b).

[95] *Id.* § 25-5.2(a)(ii).

[96] *Id.* § 25-5.2(a)(iii).

[97] *Id.* § 25-5.2(a)(iv).

legislature to select any of these three restrictions.[98] Law enforcement access to location information for a single point in time would be permissible for any legitimate law enforcement purpose.[99]

In the interest of brevity, I will not address the LEATPR Standards' postaccess provisions in this Article. The Standards are comprehensive, addressing not only law enforcement access to a record, but also notice of that access, along with the retention, maintenance, and disclosure of that record. For example, under the assumptions above, the Standards would require that law enforcement ultimately notify the cell phone customer of any access beyond a single point in time, regardless of whether the duration was less than or greater than one day.[100] Such notice would be a significant improvement to federal law.[101]

C. PROBABLE CAUSE OF WHAT?

Before turning to the administrability of the LEATPR Standards' regime, it is worth pointing out that more work should be done regarding just what constitutes relevance, reasonable suspicion, and probable cause. Although these terms have been part of the criminal procedure lexicon for years, they are surprisingly ill developed. Professor Andrew Taslitz has just recently begun the task of grappling with their meaning in the records context.[102]

Consider the Standards' language for highly protected records, which requires "a judicial determination that there is probable cause to believe the information in the record contains or will lead to evidence of crime."[103]

---

[98] Others have proposed different solutions. *See* Pell & Soghoian, *supra* note 3, at 180–83 (modeling historic access on an 18 U.S.C. § 2703(d) (2006) order and requiring a court order supported by probable cause for prospective access); *Our Principles*, DIGITAL DUE PROCESS, http://digitaldueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163 (last visited Mar. 27, 2013) ("A governmental entity may access, or may require a covered entity to provide, prospectively or retrospectively, location information regarding a mobile communications device only with a warrant issued based on a showing of probable cause.").

[99] CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS § 25-5.3(d).

[100] *See id.* § 25-5.7(b) (requiring notice "[i]f the accessed record is highly or moderately protected"). That notice "should generally occur within thirty days after acquisition," *id.*, but can be delayed, *id.* § 25-5.7(c).

[101] *See generally* Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313 (2012).

[102] *See* Andrew E. Taslitz, *Cybersurveillance Without Restraint? The Meaning and Social Value of the Probable Cause and Reasonable Suspicion Standards in Government Access to Third-Party Electronic Records*, 103 J. CRIM. L. & CRIMINOLOGY 839 (2013).

[103] CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS §§ 25-5.2(a)(i), 25-5.3(a)(i).

The final phrase, incorporating probable cause to believe the information "will lead to evidence," was added more out of an abundance of caution than as an attempt to work a substantive change to traditional probable cause analysis.[104] The addition was made during the second reading of the Standards before the ABA Criminal Justice Council, when representatives of the Department of Justice raised concerns regarding a magistrate opinion from the District of Maryland.[105] In that opinion, Magistrate Judge Susan Gauvey justified her refusal of a government request to track, via surreptitious pinging of a mobile phone for a period of thirty days, the location of the subject of an arrest warrant.[106] As to the Standards, DOJ's proffered concern was that it would be unable to use location tracking to locate a fugitive if probable cause were required. But a fugitive is committing a crime in failing to surrender to authorities, and thus the fugitive's location *is* evidence of a crime: "Had the government's request included demonstration of the fugitive status of the subject of the arrest warrant, the request would have been fairly routine."[107] The problem in the Maryland case was *not* the requirement of a particular substantive standard for the acquisition of location information, but rather the government's attempt to use inapposite authority[108] to obtain a very significant period of location information without making even a colorable attempt to articulate the need.[109] Despite denial of the government's surveillance request, the target was arrested a few days later.[110]

Under the LEATPR Standards, if the government wanted to locate a fugitive, as opposed to tracking his or her location over a significant period, the Standards would permit, among other options, a mere judicial

---

[104] For a different proposal that makes this distinction very relevant, namely the difference between reasonable suspicion and probable cause, see Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1, 17–23 (2012). I instead see the difference between those justification standards as a difference in confidence, perhaps, for example, the difference between believing there is a 30% chance there are drugs in a car and believing there is a 40% chance. Admittedly, as Andrew Taslitz explains, it is difficult to comprehend what such percentages mean when they cannot easily be tied to metaphor, *see* Taslitz, *supra* note 102, at 839, but perhaps the spectrum itself creates a metaphor in this sense: relative judgments are possible from those benchmarks for which a metaphor *is* readily available (e.g., a preponderance as a slight tipping of what were equally balanced scales).

[105] *In re* Application of the United States for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526 (D. Md. 2011).

[106] *See id.* at 530–32.

[107] *Id.* at 537.

[108] *See id.* at 536, 571–78.

[109] *See id.* at 530, 532.

[110] *See id.* at 532.

determination of relevance or a prosecutorial certification of relevance.[111] More generally, it seems reasonable for law enforcement to acquire limited location information in order to locate the target of an arrest warrant even if that target is not believed to be a fugitive,[112] and Judge Gauvey recognized that a legislature could perhaps authorize such law enforcement access.[113] It may also be reasonable if a person is merely believed to have relevant information, meaning that locating that person "will lead to evidence of crime," to use the Standards' language. More work is required to determine what probable cause should mean in the context of location information[114] and, more generally, in the context of record information. Whether it should require a fair probability[115] that information contains evidence of crime, or only a fair probability that information is relevant to an investigation of crime is a worthy topic that is beyond the scope of this Article.[116] Without that detailed analysis, it is impossible to appreciate how significantly the latter might expand law enforcement authority or to understand the benefits thereof.

D. ADMINISTRABILITY OF A "MOSAIC" APPROACH

Some commentators, foremost among them being Orin Kerr, have raised very legitimate concerns with a "mosaic" approach in which a certain law enforcement technique or access is not restricted, or has a lesser restriction, but *becomes* restricted when law enforcement engages in too much of it.[117] On the one hand, there is nothing novel in the constitutionality of law enforcement conduct depending upon the totality of law enforcement behavior and outside circumstances. This is true for such commonplace considerations as whether police conduct constitutes a Fourth

---

[111] *See supra* note 89 and accompanying text.

[112] *See In re Application*, 849 F. Supp. 2d at 558–59, 564.

[113] *See id.* at 530.

[114] This issue has been raised before, including by Magistrate Judge Gauvey and other magistrates considering requests for location information. *See id.* at 560–62 (discussing Kerr's testimony); *In re* Application of United States for an Order, 727 F. Supp. 2d 571, 580–85 (W.D. Tex. 2010) (discussing the requirements of Fed. R. Crim. P. 41 in this regard); *Location Based Technologies Hearing*, *supra* note 6, at 39–40 (2010) (testimony of Professor Orin S. Kerr); Pell & Soghoian, *supra* note 3, at 155–56 (discussing both Judge Gauvey's opinion and Kerr's testimony).

[115] *See* Illinois v. Gates, 462 U.S. 213, 238, 246 (1983) (defining probable cause to require a "fair probability").

[116] Note that in the example of Part I, placing the High Country Bandits near the robberies is evidence of crime.

[117] *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320 (2012).

Amendment seizure requiring reasonable suspicion,[118] whether police conduct constitutes a de facto Fourth Amendment arrest requiring probable cause,[119] or whether a suspect is in "custody" such that *Miranda* warnings are required.[120] Sometimes drawing a firearm will elevate a stop into a de facto arrest and *Miranda* custody; other times it will be permissible as part of a limited *Terry* stop.[121] And sometimes constitutionality, or at least admissibility, depends upon what other officers have done, such as the impact of an invocation of the *Miranda* right to counsel in an unrelated interrogation.[122] And courts have long recognized the relevance of the potential for large amounts of particular information to create a virtual current biography of an individual.[123] Nonetheless, there is something potentially novel, and certainly important, when it comes to tiered restrictions on accessing location information.

Consider the proposal of the last section: accessing a record containing more than a day of location information requires a court order resembling a warrant, but accessing a day or less requires a lesser court order. Imagine that an officer investigating a bank robbery wants to obtain the cell phone location information of a suspect for the three-hour block surrounding the robbery. Three hours are, of course, less than twenty-four, so a lesser court order would seem sufficient. However, must the officer scour his or her existing file to ensure that location information was not previously requested? If twenty-two hours of location information were previously requested, does this put the new request "over the top," meaning a warrant is required? Does the officer also have to check with fellow officers in the department to see what they have obtained? With other departments? How long does a previous access remain relevant? Does an access six days ago "count"? Six weeks? Six years?[124]

---

[118] *See* United States v. Drayton, 536 U.S. 194, 202 (2002) (asking "whether a reasonable person would feel free to decline the officers' requests or otherwise terminate the encounter") (internal quotation marks omitted).

[119] *See* Dunaway v. New York, 442 U.S. 200, 212–13 (1979) (looking to movement, show of authority, and duration in differentiating a de facto arrest from a *Terry* stop).

[120] *See* Berkemer v. McCarty, 468 U.S. 420, 440–42 (1984) (defining custody as when a reasonable person would feel her freedom of movement had been curtailed to the degree associated with a formal arrest).

[121] *See* United States v. Hensley, 469 U.S. 221, 224, 234–36 (1985) (holding that detention was a *Terry* stop despite drawing of service revolver).

[122] *See* Arizona v. Roberson, 486 U.S. 675, 682–85 (1988) (holding invocation effective as against a different officer unaware of it).

[123] *See, e.g.*, Burrows v. Superior Court of San Bernardino Cnty., 529 P.2d 590, 596 (Cal. 1974) (recognizing that "the totality of bank records provides a virtual current biography").

[124] Orin Kerr refers to this as the "duration and scale" "grouping" problem, and it strikes me as the only truly novel circumstance of what he terms the mosaic approach. *See* Kerr, *supra* note 117, at 333–34. I tend to think "grouping" across investigatory methods would

Clearly a system that takes into account past requests in this manner, at least without significant limitation, is not reasonably administrable. At the same time, we would not want to permit an officer to game the system: desiring three days worth of location, she requests twenty-four hours of location on day one, the subsequent twenty-four hours on day two, and the final twenty-four hours on day three, each time using the lesser restraint applicable to shorter duration requests. In order to accommodate these competing concerns, I would as a rule *not* require police to consider past requests. If an officer seeks to obtain twenty-four hours or less of location information, the lesser process requirement applies. However, if a court finds the lesser process has been abused, appropriate sanctions should kick in, potentially including suppression in any future criminal prosecution, administrative discipline, civil penalties, and even criminal sanctions if the violation were willful.[125]

An "abuse" trigger is not as easy to predict and administer as a bright-line rule. Rather, it is a standard that will require some discretion in its application, and at least until there is ample judicial precedent, there will be some uncertainty on the margins. But it should provide adequate guidance to law enforcement officers investigating in good faith, and it will achieve the right result most of the time.

There remains a lingering ambiguity. Imagine an officer wants to obtain a suspect's location for a single hour of the day (say, 9:00 a.m. to 10:00 a.m.) for a period of two weeks. Is a record containing that information, using the terms of the LEATPR Standards, highly or moderately protected? In other words, does this count as fourteen hours of location information, and therefore the record is moderately protected, or does this count as over twenty-four hours of location information because it pertains to many days? My preference would be to simply count the hours, since time is typically the best measure of invasiveness with regard to location information. Thus, I would consider such a record moderately protected. Reasonable minds can disagree; what is critical is that a decisionmaker considers and carefully delineates which rule would apply.

E. APPLICATION TO THE HIGH COUNTRY BANDITS

The High Country Bandits committed sixteen bank robberies. If police

---

not be worth the candle. *See id.* at 335–36.

[125] The LEATPR Standards do not take a position on particular sanctions for particular violations, instead providing only that "[t]he 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." CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS § 25-7.1 (2012).

were content to obtain an hour of cell tower information for each robbery, or several hours of information for several robberies, that would be less than my posited twenty-four-hour threshold. Thus, under the LEATPR Standards, the information might be moderately protected. But even those lesser restrictions could not be satisfied. If the police had a suspect, they could obtain the information for that suspect. But the police had no suspect. Instead, when police in the actual investigation obtained cell tower information for four of the robberies, they obtained information on 150,000 different subscribers.[126] Quite obviously, almost all of those persons were entirely innocent of the crime. Assuming only two robbers, which was the actual case, at least 99.999% of them were innocent. Assuming a large group of ten robbers, at least 99.993% of them were innocent. Therefore, as to the record pertaining to each of those 150,000 subscribers, even a relevance threshold was not satisfied. Relevance is a very low substantive standard, but it is nonetheless being used as a standard of individualized suspicion. That *some* subscribers' records are relevant to an investigation does not permit police to obtain *all* subscribers' records.[127]

I earlier asserted that this acquisition of cell tower dumps was good police work; using this technique police were able to solve serious crime that was otherwise potentially unsolvable.[128] Does this mean that we must reduce the level of protection given to location information? Because, in the Standards' words, police are "unable to solve . . . an unacceptable amount of otherwise solvable or preventable crime, such that the benefits of respecting privacy are outweighed by this social cost"?[129] Fortunately, there is a better way that does not require this privacy hit, and that is working with de-identified records.

F. DE-IDENTIFIED RECORDS AND THE HIGH COUNTRY BANDITS

The LEATPR Standards relate to law enforcement access to third-party records, where a record is defined as follows: "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.

---

[126] *See supra* note 2 and accompanying text.

[127] In other words, imagine police believe a bank customer is engaged in money laundering. Quite obviously that does not mean that the records of *all* bank customers are relevant to that investigation merely because that vast swath of information will happen to include relevant information. Otherwise, every record in existence would be "relevant" to a criminal investigation for which they were *all* requested.

[128] *See supra* Part I.A.

[129] CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS § 25-4.2(b).

A 'de-identified record' contains information that is not so linkable."[130]

There are important developments in the computer science and law of de-identification, and those will be addressed in the Standards Commentary. But for our purposes it is sufficient to understand that a "reasonable efforts" standard 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. The danger of re-identification is very significant when purportedly de-identified data will be accessible to the public. But where the data will merely be accessible to law enforcement in furtherance of a criminal investigation, and where that access, re-identification, retention, and future disclosure are all subject to other constraints, the danger is far less significant. Thus, the particular manner of de-identification need not be as robust as in other contexts.

What might constitute de-identification with respect to a cell tower dump? The phone provider could simply replace every unique phone number with a code. So, if the phone company records appeared as in Tables 1 and 2, the de-identified records might appear as in Tables 3 and 4. The only critical criterion for the labels is that where a phone number appears more than once (in this case (899) 776-6369), it must of course be given the same de-identified label every time (in this case C). For hundreds of thousands of records the labels will appear more complicated, but the concept remains the same.

Table 1

Cell Tower 95-1300

Registering Phone	**Time**
(855) 943-3821	9:32
(844) 139-4185	9:33
(899) 776-6369	9:35
(855) 384-5528	9:35
(833) 728-6401	9:36

[130] *Id.* § 25-1.1(g).

Table 2
Cell Tower 48-2700

Registering Phone	Time
(822) 868-7328	14:07
(899) 024-2182	14:07
(844) 412-9589	14:08
(899) 776-6369	14:08
(899) 546-5222	14:10

Table 3
De-Identified Cell Tower 95-1300

Registering Phone	Time
A	9:32
B	9:33
C	9:35
D	9:35
E	9:36

Table 4
De-Identified Cell Tower 48-2700

Registering Phone	Time
F	14:07
G	14:07
H	14:08
C	14:08
I	14:10

What would the Standards require of law enforcement in order to obtain such de-identified records? According to Standard 25-5.6(a), "law enforcement should be permitted to access an appropriately inclusive body of de-identified records . . . pursuant to an official certification." The Standards require an "appropriately inclusive" set of records in order to leverage the checks of the political process, and that is achieved where the data includes every active cell phone for a number of different cell towers. Persons of power and influence are potentially subject to this intrusion, and therefore we can expect it to be the subject of debate and oversight.[131] An official certification requires "a written determination by a politically accountable official that there is a reasonable possibility that the record is

[131] *See id.* § 25-5.7(e) (requiring notice for the access of de-identified records).

relevant to initiating or pursuing an investigation."[132] Not only is the reasonable possibility threshold a very low one, but here the Standards are specifically meant to permit searching through the haystack in order to find the relevant needle, and therefore would permit the transfer in the investigation of the High Country Bandits.[133]

What would law enforcement do with the de-identified records? Although in some circumstances algorithmic searches will be quite complicated, in this instance it is very simple: compare the different cell tower dumps to determine whether a certain de-identified label or labels are present in multiple lists. Although the data was not de-identified, this is otherwise precisely what FBI special agents did. The tower dump information was entered into Microsoft Access, and the resulting tables "were then queried for any cell phone numbers that were common between the different robbery dates and cell tower locations."[134] Using the hypothetical de-identified data of Tables 3 and 4, law enforcement will find a "hit" for cell phone "C." Indeed, rather than complete the transfer, a phone provider might run the query in its own records and report only whether there was a "hit." That selective revelation is exactly what the Standards are attempting to achieve via de-identification.

The officers now have only a placeholder, rather than a phone number. On what basis can they re-identify the data, i.e., learn from the phone provider the number for phone "C"? Standard 25-5.6(b) provides, "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."[135] In this instance, the record reflects location at a particular time. Thus, if location information is moderately protected, then re-identification requires satisfying the same standards for accessing moderately protected information described above. In the High Country Bandits investigation, a prosecutor could demonstrate either relevance or reasonable suspicion to a court, as demonstrated by the criminal complaint:

> [D]ue to the vast difference in distance and time between the cell towers and the dates of the robberies, investigators believed that it would be extremely unusual for a cell

---

[132] *Id.* § 25-5.2(c).

[133] Admittedly, we probably could have done a better job in the blackletter of differentiating the typical individualized relevance standard from this global reasonable possibility of relevance standard. Fortunately, the entire design of the de-identification provisions makes any other interpretation impossible.

[134] Criminal Complaint, *supra* note 9, at 14.

[135] CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS § 25-5.6(b).

> phone number to appear on two or more of the cell phone towers servicing the area of the bank[s] on the exact robbery dates.[136]

For this process to function, third parties must be willing to perform the requested de-identification, and thus a legislature enacting the Standards might want to include such a requirement and reimbursement for costs. But what if a third party is simply unable to perform the requested de-identification, or at least unable to do so without very significant expense? It is within the spirit of the Standards to permit other alternatives that accomplish the same ends. For example, in 2005, police in Rotterdam, Netherlands, wanted to identify those involved in a riot.[137] They obtained from phone providers 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.[138] 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 sole 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 the Standards.[139]

To the contrary was a law enforcement request that was recently denied in the Southern District of Texas.[140] Magistrate Judge Brian Owsley rejected four applications for cell tower dumps in which neither the prosecutor nor the special agent seemed to understand the relevant

---

[136] Criminal Complaint, *supra* note 9, at 13–14. Neither reasonable suspicion nor the more demanding probable cause requires precise quantification of probability. *But see* Erica Goldberg, *Getting Beyond Intuition in the Probable Cause Inquiry*, 17 LEWIS & CLARK L. REV. (forthcoming 2013) (manuscript at 48–49) (arguing that a precise probability should be determinative when it *can* be calculated).

[137] *See* BRUCE SCHNEIER, SCHNEIER ON SECURITY 28 (2008).

[138] The Standards require ultimate deletion of all de-identified records. *See* CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS § 25-6.1(c).

[139] The text message actually used by Rotterdam police may have been deficient. *See* David Rennie, *Dutch Hooligans Rounded up by Text*, TELEGRAPH (Sept. 1, 2005, 12:01 AM), http://www.telegraph.co.uk/news/worldnews/europe/netherlands/1497387/Dutch-hooligans-rounded-up-by-text.html (describing it as a "terse message . . . informing users that they were known to have been in the vicinity").

[140] *In re* Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d) Directing Providers to Provide Historical Cell Site Location Records, C.R. Nos. C-12-670M–673M, 2012 WL 4717778, at *4 (S.D. Tex. Sept. 26, 2012).

technology, there was no coherent explanation of how the data would be used to identify the perpetrator, and there was no promise to ignore and then destroy irrelevant data.[141] Quite obviously the LEATPR Standards provide a better solution.

III. REAL-TIME LOCATION SURVEILLANCE

Part II describes how the ABA LEATPR Standards would apply to law enforcement accessing historic location information from a private service provider in nonexigent and nonconsensual circumstances.[142] The Standards do not apply to real-time surveillance by a law enforcement officer, either via the naked eye or with the assistance of technology.[143] However, the initial default position should be the same level of restriction, because the law enforcement need and the privacy intrusion are the same. Whether police receive my location information as I "create" it or a week later, assuming the same level of detail for both, the information—and therefore the benefit to law enforcement and the privacy implications—are identical. Thus, it is not surprising that requests for wiretaps (real-time surveillance) are plummeting now that police often have alternative means of acquiring the same or equivalent information that are statutorily less restricted.[144] That differentiation is a mistake; Fourth Amendment and statutory restrictions should typically be the same for real-time and historic access.

Thus, for real-time location tracking that is technologically assisted, as via a GPS tracking device or a drone, the same standards developed above should apply. Under the developed assumptions, law enforcement tracking for more than a day would require a warrant supported by probable cause; nonexigent law enforcement tracking for less than a day would require a lesser court order.[145] There might also be apt analogues to de-identified historic access. For example, if unmanned aerial vehicles are used to monitor a multiday protest, perhaps—as with airport screeners—they can be configured to eliminate personally identifying details, showing only generic body shapes, unless and until such details become relevant.[146] On

---

[141] *See id.* at *1, *4.

[142] It should be stressed that the relevant consent is *not* that of the service provider but rather is that of the subscriber. *See* CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS § 25-5.1.

[143] *See id.* § 25-2.1(e).

[144] *See* Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1322–25 (2012); Lichtblau, *supra* note 34.

[145] There would not seem to be an equivalent to obtaining a store receipt that reveals location at only a single point in time.

[146] *See* Katie Johnston, *A Modest Solution: TSA Is Replacing Body Scanners that Drew Privacy Complaints*, BOS. GLOBE, Oct. 5, 2012, at B5, B8 (describing privacy-protective airport screeners); Joe Sharkey, *A Farewell to 'Nudity' at Airport Checkpoints*, N.Y. TIMES,

the other hand, even such "de-identified" aerial observation could be intimidating and have a chilling effect on First Amendment protected activity. There are many issues to work through, and for now as to real-time surveillance I am content to begin the construction of a potential framework.[147]

What of real-time location surveillance that is not technologically assisted? My default is of course equal treatment for real-time and historic access. And because the privacy intrusion is tied to the *amount* of location information much more fundamentally than to the means of gathering, my preference, like that of Christopher Slobogin, is to vary the regulation solely by time.[148] But the default of equal treatment for real-time and historic access should be trumped when there is good reason, and in this instance there is a terrific reason. It would be devastating to legitimate law enforcement, and even downright silly, if a police officer had to get a court order before looking at a person and thereby determining his or her location.

So, what restraint should apply to visual surveillance by the naked eye? My tendency is to permit police the lesser period of visual surveillance, twenty-four hours or less, without restraint.[149] More precisely, the only restraint would be that which applies to all law enforcement conduct, namely that there be some legitimate law enforcement purpose.[150] This would include purposes as diverse as training and "staying current" in order to be aware of potential needs for law enforcement assistance, but

---

Jan. 22, 2013, at B6 (describing removal of intrusive screeners from airports).

[147] A typical consideration is that technologically assisted police surveillance is of greater concern because technology eliminates previously significant resource restraints on prolonged surveillance. As explained by Justice Alito in *United States v. Jones*:

> 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.

132 S. Ct. 945, 963–64 (2012) (Alito, J., concurring in the judgment). The elimination of former resource restraints is most relevant if the baseline is no restriction. Because my proposal would restrain law enforcement location surveillance even if not technologically assisted, this resource distinction is much less important.

[148] *See* Slobogin, *supra* note 104, at 24–27, 35.

[149] Slobogin's solution is the same but more restrictive, limiting "targeted public" viewing of persons to twenty minutes without a court order. *See id.* at 25, 27. He of course recognizes an exception for exigent circumstances. *See id.*

[150] *See* CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS § 25-5.3(d) (2012).

would not, for example, include following a particularly attractive person. One could reasonably argue that the twenty-four hours is too long a period to be without court regulation, especially when spread into single-hour intervals over many days, in which case perhaps the limit should instead be twelve hours. Either way, longer periods of surveillance would require additional restraint, and here I would apply the default same-as-historic rule. Thus, surveillance longer than twenty-four hours would require a court order supported by probable cause. If a jurisdiction were to adopt the lesser period of unregulated visual surveillance, then surveillance of more than twelve hours up to twenty-four hours would require a lesser court order. These two options are depicted in Tables 5 and 6.

Table 5
Visual Surveillance Option 1

Duration	**Regulation**
≤ 24 hours	Legitimate law enforcement purpose
> 24 hours	Warrant

Table 6
Visual Surveillance Option 2

Duration	**Regulation**
≤ 12 hours	Legitimate law enforcement purpose
12 hours < duration ≤ 24 hours	Lesser court order
> 24 hours	Warrant

Under this construct we once again have the mosaic concern. Can an officer look upon this person today if the officer watched him or her last week? I would resolve the concern in the same manner as for historic surveillance. Law enforcement can engage in independent twenty-four-hour (or twelve-hour) periods of surveillance without restraint; if a court finds an abuse of this no-court-order process, appropriate sanctions should apply.

This works a change in traditional Fourth Amendment law: the Supreme Court "has to date not deviated from the understanding that mere visual observation does not constitute a search."[151] But that is a history that has always been wanting and that has received very little development by the Court. Naked-eye surveillance is sufficiently intimidating that we regulate it via the laws of harassment and stalking, and as Christopher Slobogin, Andrew Taslitz, and others have developed, it certainly affects

[151] *Jones*, 132 S. Ct. at 953.

the security of our persons.[152] While I thus strongly believe that there should be Fourth Amendment restriction on extended stakeouts and undercover operations, there can of course be legislative and administrative restraints even in its absence.

A legislature, police officer, or court determining "abuse" will have to confront some nuanced issues that, at least as matters of first impression, might be difficult. For example, say an officer is watching over a park during a multiday "Occupy" protest.[153] Must the officer obtain a warrant because he is likely to view the same person over multiple days and realizes this in advance? I would think not, just as I would not require a court order when an officer executing his rounds realizes he will see the same persons at the same locations day after day because they too are going about their predictable daily routines. But how is the law to demarcate such permissible surveillance from impermissible long-term surveillance?

We have already seen a solution, only it does not work for naked-eye visual surveillance: we would like to de-identify the information, and permit access to appropriately inclusive bodies of such de-identified information subject only to the checks of the political process.[154] We are not concerned about police happening to see certain persons in the performance of their duties, but we do not want them watching a single person or home over a long period without judicial preclearance. Because we cannot "de-identify" persons whom an officer sees—we cannot program eyeballs to only see bodily outlines, for example—we need an alternative basis for differentiating the unrestricted from the restricted that will get much the same result. Perhaps the question to ask is whether a reasonable officer would believe the police were systematically collecting information regarding a particular individual or individuals. If so, and if that information will be location information for more than twenty-four hours (or twelve hours under Option 2 (see Table 6)), police must seek a court order. If not, then the conduct is permissible for any legitimate law enforcement purpose. Christopher Slobogin has proposed essentially this

---

[152] *See* Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 237–251 (2002); Andrew E. Taslitz, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions*, 65 LAW & CONTEMP. PROBS. 125, 169–74 (2002). Visual surveillance is regulated in other countries. *See* Susan Freiwald & Sylvain Métille, *Reforming Surveillance Law: The Swiss Model*, BERKELEY TECH. L.J. (forthcoming 2013) (manuscript at Sec. G (Physical Observations)).

[153] *See* Michael S. Schmidt, *For Occupy Movement, a Challenge to Recapture Momentum*, N.Y. TIMES, Apr. 1, 2012, at A21.

[154] For an explanation of the benefits of process, see Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 554–59 (2005).

solution, where he differentiates between "general" and "targeted" searches.[155]

Because for years we have had little to no restriction on law enforcement naked-eye observation, momentum favors something like this model. Visual surveillance for some period is restrained only by the requirement of a legitimate law enforcement purpose; technologically assisted surveillance for that period is regulated just like that same period of historic records access. Visual surveillance, technologically assisted surveillance, and historic records access for a longer period all receive the same greater restraint.

IV. A FEW THOUGHTS ON PROCESS

Scholars are now crafting specific proposals in the wake of *United States v. Jones*, and in some sense this task will never be complete. No matter what the courts and legislatures decide, there will be room for improvement, and changing technologies and social norms require changing laws.[156] Naturally, better solutions require robust and open participation and debate, and a critical component is active and engaged participation by law enforcement.[157] This is not to say that law enforcement is the only

---

[155] Slobogin, *supra* note 104, at 16–32. "A *targeted search* seeks to obtain information about a specific person or circumscribed place. A *general search* seeks to obtain information about people or places that are not targets at the time of the search." *Id.* at 17. The Swiss system makes a similar differentiation. *See* Freiwald & Métille, *supra* note 152.

[156] Although commentators disagree on what the solution should be, we seem united in recognizing that changing technologies require reevaluation of existing rules. *See, e.g.*, Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011) (arguing that the courts have traditionally recalibrated Fourth Amendment rules to account for changing technologies); Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 619 (2011) (arguing for a principle of "technosocial continuity" in which "courts consider both the ways in which technology facilitates intrusive surveillance and the ways in which technology spurs social change that may make citizens more vulnerable to existing surveillance technologies").

[157] For a helpful account of some instances in which engaged debate has improved security and privacy, see Jeffrey Rosen, *Naked Scanners, GPS Tracking, and Private Citizens: Technology's Role in Balancing Security and Privacy*, 57 WAYNE L. REV. 1 (2011). Kurt Schmid, Executive Director of the Chicago High Intensity Drug Trafficking Area Program, points out a slightly different way in which dialogue can benefit law enforcement:

> The law enforcement community has repeatedly learned that the criminal quickly adapts new technologies to his repertoire of tools not only to enhance his illicit activities, but also to create—and we hope only a temporary—safe haven in which to operate. Law enforcement, generally lagging the technological capability and/or the legal precedent to intercept or access communication and data, must deal with these difficult situations for sometimes long periods of time before solutions are found. Opportunities to sit at the table with industry, privacy advocates, and lawmakers prior to major technology rollouts are crucial to preventing sometimes years of unintended consequences.

critical participant in the discussion. For example, Andrew Taslitz urges the participation of those governed by, and particularly those most affected by, police conduct.[158] But because the law enforcement community sometimes seems hesitant or even unwilling to participate in this conversation, I comment briefly upon that need.

In order to draft the ABA LEATPR Standards, it was essential to hear from representatives of law enforcement. Although there were absolutely differences of opinion on precisely where to draw the privacy versus safety line, most often the differences instead concerned whether a particular proposal would affect that line. This is something that is impossible to know without input from both "sides," meaning from law enforcement officers and prosecutors on one side, and from defense attorneys and privacy advocates on the other. Theory is wonderful, and as law professors we engage in a great deal of it, but we—or at least most of us—ultimately hope to ground that theory by carefully considering how it will apply in the real world. This requires knowing as much as possible about everyday events and policing.

In some countries police might actively press legislative discussion because it suits their law enforcement interest: the default is that they *cannot* use an investigative procedure, meaning that absent affirmative legislative authorization, police are not permitted to so operate.[159] Because the default in the United States is the contrary, permitting police to do what the legislature has not prohibited, there is an understandable tendency among some in law enforcement to avoid drawing attention to tactics that might, if considered, be regulated. Of course, any search or seizure can be constitutionally regulated, and perhaps there is a slightly greater risk of such constitutional regulation if a legislature does not step in first. But that is a slight risk, and an American officer might plausibly figure that an investigative technique that does not draw attention will not draw regulation, and that allows for getting more bad guys and gals off the

---

ECPA Reform and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. 111–49 (2010) (testimony of Kurt F. Schmid, Director, Chicago High Intensity Drug Trafficking Area Program).

[158] *See* Andrew E. Taslitz, *The Criminal Republic: Democratic Breakdown as a Cause of Mass Incarceration*, 9 OHIO ST. J. CRIM. L. 133 (2011) (arguing that real deliberative processes increase public support for the justice system and foster more pragmatic, less punitive responses); Andrew E. Taslitz, *Fourth Amendment Federalism and the Silencing of the American Poor*, 85 CHI.-KENT L. REV. 277 (2010) (arguing for increased participation by poor racial minorities); Andrew E. Taslitz, *Racial Auditors and the Fourth Amendment: Data with the Power to Inspire Political Action*, 66 LAW & CONTEMP. PROBS. 221 (2003) (arguing for "racial auditing" as a method of police regulation).

[159] *See, e.g.*, Freiwald & Métille, *supra* note 152 (describing the Swiss default).

streets, which keeps us all safe. As a criminal analyst for the state of Iowa said about cell phone location tracking, "We find people, and it saves lives."[160]

Thus, the Iowa City Police Department warns officers to keep cell phone tracking out of reports, and further cautions as follows: "Do not mention to the public or the media the use of cellphone technology or equipment used to locate the targeted subject."[161] In a provocative recent article, federal Magistrate Judge Stephen William Smith of the Southern District of Texas explains how the current system of sealing government surveillance requests severely limits our understanding of what is taking place:

> Through a potent mix of indefinite sealing, nondisclosure (i.e., gagging), and delayed-notice provisions, . . . 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.[162]

Quite obviously such lack of information is not conducive to the best minds being able to deliberate the best solutions, and hopefully law enforcement can increasingly be persuaded to bring to the table their expertise and experiences, such that all of the relevant actors—from the police to the courts to the legislatures to the academics—will have more information. Ideally law enforcement will actively seek legislation that provides the authorization they require, rather than seek to operate in its absence. At the very least, we can hope to do better than the view expressed by Governor Lincoln Chafee of Rhode Island in vetoing a law restricting law enforcement searches of cell phones. "The courts," claimed Governor Chafee, "and not the legislature, are better suited to resolve these complex and case specific issues."[163] It is a particular shame to see an

---

[160] Eric Lichtblau, *Police Are Using Phone Tracking as a Routine Tool: Cell Companies Profit*, N.Y. TIMES, Apr. 1, 2012, at 1.

[161] *Id.* For a complementary view that police are reticent to discuss these techniques, see Pell & Soghoian, *supra* note 3, at 158.

[162] Smith, *supra* note 101, at 602.

[163] Letter from Lincoln D. Chafee, Governor, to Speaker of the House of Representatives (June 25, 2012), *available at* http://www.governor.ri.gov/documents/Vetoes/Veto Message 12-H 7110.pdf; *see also* Sengupta, *supra* note 87, at A1. Governor Jerry Brown of California expressed the same sentiment in vetoing a similar California law. *See* Amy Gahran, *California Governor Allows Warrantless Search of Cell Phones*, CNN (Oct. 11, 2011, 12:31 PM), articles.cnn.com/2011-10-11/tech/tech_mobile_california-phone-search-veto_1_cell-phones-smartphone-text-messages ("The courts are better suited to resolve the complex and case-specific issues relating to constitutional search-and-seizures protections.") (quoting Governor Brown's statement).

executive declare such a backwards theory when his legislature had acted; legislatures far too often abdicate their role, leaving the regulation of criminal investigations to the courts' constitutional analysis in the first instance.

V. CONCLUSION

My colleague Joseph Thai and I run a service for criminal law and procedure professors in which we gather, categorize, analyze, and make available multimedia materials for classroom use.[164] We often regret that so much of the material chronicles bad law enforcement behavior. While there is certainly much to learn from such mistakes, focusing solely on mistakes does a disservice to the many conscientious law enforcement agents around the country who are actively working not only to remain within the law, but to act in the best spirit of that law. But for obvious reasons such praiseworthy conduct is less likely to be chronicled in the news, and thus we are beginning to actively seek it out. It is in that same vein that I consider the investigation of the High Country Bandits chronicled in this Article. It is an example of terrific police work. By developing a system of thoughtful regulation that takes advantage of de-identification, this Article demonstrates that we can permit such investigation and very effectively protect our privacy, making us secure in our persons, houses, papers, and effects, and thus fulfilling the promise and purpose of the Fourth Amendment. If we can encourage police to participate actively in dialogue and to be more than reactive in the legislative process, it is possible to achieve the twin aims of safety and privacy that bring security.

While obviously I find value in the particular solutions I proffer for regulating law enforcement access to location information, the most significant value of the ABA LEATPR Standards is their provision of a thoughtful framework through which interested parties can arrive at their own desired solution. I encourage decisionmakers at all levels and in all roles—police departments, prosecutors' offices, legislatures, and courts—to take advantage of that framework as they make the difficult decisions of how best to regulate law enforcement access to information in the era of Big Data.[165]

---

[164] THE CRIMPROF MULTIPEDIA, http://jackson.law.ou.edu/criminal (last visited Mar. 27, 2013).

[165] *See* Dennis Overbye, *Mystery of Big Data's Parallel Universe Brings Fear, and a Thrill*, N.Y. TIMES, June 5, 2012, at D3.