CAUSE TO BELIEVE WHAT? THE IMPORTANCE OF DEFINING A SEARCH'S OBJECT—OR, HOW THE ABA WOULD ANALYZE THE NSA METADATA SURVEILLANCE PROGRAM

CHRISTOPHER SLOBOGIN*

Courts and scholars have devoted considerable attention to the definition of probable cause and reasonable suspicion. Since the demise of the "mere evidence rule" in the 1960s, however, they have rarely examined how these central Fourth Amendment concepts interact with the "object" of the search. That is unfortunate, because this interaction can have significant consequences. For instance, probable cause to believe that a search "might lead to evidence of wrongdoing" triggers a very different inquiry than probable cause to believe that a search "will produce evidence of criminal activity." The failure to address the constraints that should be imposed on the object of a search has particularly acute implications in the context of records searches. This article explores the ramifications of this gap in Fourth Amendment jurisprudence both generally and in connection with the NSA's metadata program, with particular attention to how the American Bar Association's Standards on Law Enforcement Access to Third Party Records, the topic of this symposium, resolve the relevant issues.

Recent disclosures prompted by former National Security Agency analyst Edward Snowden's revelations have corroborated earlier allegations that the NSA has, for at least the past seven years, been collecting and analyzing vast amounts of domestic as well as foreign communications information.[1] Some allege that the NSA is accessing the *content* of all phone and email communications, not just from foreign sources but from *domestic* sources as well.[2] The NSA has not owned up to that practice, but

---

* Milton Underwood Professor of Law, Vanderbilt University Law School. The author was on the Task Force that drafted the American Bar Association's CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS. *See infra* note 5.

1. Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, WASH. POST, Oct. 14, 2013, at A1.

2. Glenn Greenwald, *XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet"*, GUARDIAN (July 31, 2013, 8:56 AM), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data ("A top secret National Security Agency program allows analysts to search with no prior authorization through vast databases

it has admitted to storing telephonic metadata—that is, the anonymous envelope or transmittal information associated with phone calls—in connection with virtually every call made in or through the United States.[3] Further, it has conceded that it is subjecting this metadata to "queries" meant to identify those who communicate with "seed identifiers" who are thought to be connected to terrorist or other clandestine threats to national security.[4]

One goal of this essay is to analyze how the American Bar Association's Criminal Justice Standards on Law Enforcement Access to Third Party Records (LEATPR Standards), the provisions that are the subject of this symposium, would regulate the NSA's metadata program.[5] The LEATPR Standards make clear in their very first substantive provision that they do not apply to "access[ing] . . . records for purposes of national security."[6] But the NSA program is representative of a number of other domestic law enforcement efforts—for instance, the seventy-plus "fusion centers" that have been set up to collect and fuse together information from public and private sources—that also involve government accumulation of vast amounts of data.[7] Because, thanks to Snowden, we know as much or more about the NSA's program as these other programs, the NSA's collection of metadata is a useful springboard for discussing how the Standards would work in these routine criminal investigation contexts.

The second, and more fundamental, goal of this essay is to elucidate a much neglected aspect of surveillance law and of Fourth Amendment jurisprudence generally. Under the Fourth Amendment, most searches require probable cause, but some searches or "search-like" activities require

---

containing emails, online chats and the browsing histories of millions of individuals, according to documents provided by whistleblower Edward Snowden.").

3. *See* David S. Kris, *On the Bulk Collection of Tangible Things*, LAWFARE RES. PAPER SERIES, Sept. 29, 2013, at 6 & n.24, http://www.lawfareblog.com/wp-content/uploads/2013/09/Lawfare-Research-Paper-Series-No.-4-2.pdf (describing government's declassification of an order from the Foreign Intelligence Surveillance Court authorizing the metadata collection and the government's additional disclosures about the program).

4. *See id.* at 10 & n.41.

5. CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS (2013). Individual standards will be referred to using the format 'STANDARD x-x.'

6. STANDARD 25-2.1(a).

7. For a description of fusion centers, see THE CONSTITUTION PROJECT, RECOMMENDATIONS FOR FUSION CENTERS: PRESERVING PRIVACY AND CIVIL LIBERTIES WHILE PROTECTING AGAINST CRIME AND TERRORISM 4-7 (2012), *available at* http://constitutionproject.org/pdf/fusioncenterreport.pdf. *See also* Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 317-321 (2008) (describing a number of "large-scale" federal data mining programs).

a lesser threshold such as reasonable suspicion.[8] These justificatory concepts—what this essay will call "standards of proof"—are ambiguous in and of themselves, as many have pointed out.[9] But a further ambiguity, one that has received little attention in either case law or scholarship, is how these concepts relate to what this essay will call "the object" of the search. For instance, probable cause to believe that a search *might lead* to evidence of *wrongdoing* triggers a very different inquiry than probable cause to believe that a search *will produce* evidence of *criminal activity*.[10] While the latter language requires a fair degree of certainty that solid evidence of crime will result from the search, the former standard might permit a much wider ranging exploration, which could be aimed at finding even the most circumstantial proof of minimally harmful conduct. Yet in recent times very few courts or scholars have recognized this distinction, much less explored its implications for Fourth Amendment or statutory law.[11]

This failure to address the constraints that should be imposed on the object of a search or seizure has particularly acute repercussions in the context of records searches. Records sought by the government often contain no evidence of wrongdoing or only very tangential evidence of it, a fact known by the government at the time it seeks the records. For instance, the NSA staff that runs the metadata program knows that only a very small percentage of the records subjected to its bulk collection procedure—which accesses the communication logs of virtually everyone in the country—will produce evidence of even mundane criminal activity, much less terrorism.[12] The staff also knows that even those records that are linked to a terrorist

---

8. *See* Safford Unified School District #1 v. Redding, 557 U.S. 364, 370 (2009) ("The Fourth Amendment 'right of the people to be secure in their persons . . . against unreasonable searches and seizures' generally requires a law enforcement officer to have probable cause for conducting a search" (citation omitted)); United States v. Sokolow, 490 U.S. 1, 7 (1989) (noting that "reasonable suspicion" is required for a stop and stating that "the level of suspicion required for a *Terry* stop is obviously less demanding than that for probable cause"); *see also* 18 U.S.C. § 2703(d) (2012) (requiring "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation").

9. *E.g.*, Bruce A. Antkowiak, *Saving Probable Cause*, 40 SUFFOLK U. L. REV. 569, 588 (2007) (noting several authors and justices who have concluded that "because attempts to define or describe probable cause produce variable, ambiguous, and shifting meanings over time, the term evades definition").

10. *See infra* Part I.

11. *See infra* text accompanying notes 40-49.

12. *See* Spencer Ackerman, *NSA Review Panel Casts Doubt on Bulk Data Collection Claims*, GUARDIAN (Jan. 14, 2014), http://www.theguardian.com/world/2014/jan/14/nsa-review-panel-senate-phone-data-terrorism.

will usually end up being useless in the quest to protect national security.[13] At most, the NSA's queries will uncover the identity of someone who has communicated with a known terrorist; much more investigation, either of the content of the communication or of other social network information, must be conducted before anything evidential will be discovered.

The same scenario can arise in routine criminal investigations. Assume police suspect Mr. X of committing an armed robbery. Phone records, bank records, travel records, and a host of other documentary sources might be relevant to their investigation if, for instance, police want to establish Mr. X's location at a particular time, discover the items he bought before the robbery, or identify the people he may have contacted around the time it occurred. Arguably, it is not only important to figure out the likelihood that these types of records will be discovered (the standard of proof issue) but also the likelihood that the information in those records will be useful to the government's case (the search object issue). Even if, as the Supreme Court seems to think, the Fourth Amendment does not protect most records containing personal information when they are in the possession of third parties,[14] these types of issues need to be resolved in connection with statutory enactments and administrative practice.[15]

This essay first explicates, in Part I, the nuanced ways in which the object of a search can be conceived and how the object of a search interacts with the justification for it. Part II then addresses how the LEATPR Standards deal with this issue, particularly in the context of the NSA metadata program. Finally, Part III makes some suggestions for improving the analysis, based on other work I have done.

---

13. The NSA claims that it has foiled over fifty terrorist attacks worldwide. Kimberly Dozier, *NSA: Surveillance Programs Foiled Some 50 Terrorist Plots Worldwide*, ASSOCIATED PRESS (June 18, 2013), *available at* http://www.huffingtonpost.com /2013/06/ 18/nsa-surveillance_n_3460106.html. That figure is probably a gross exaggeration. *See* Klayman v. Obama, No. 13-0851, 2013 WL 6571596, at *26 n.65 (D.D.C. Dec. 16, 2013) (citing sources disputing this claim and noting that the government had failed to provide evidence supporting it despite an *in camera* opportunity to do so). Whatever number is correct, it is dwarfed by the thousands of queries the government conducts.

14. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 744 (1979) ("When he used his phone, petitioner voluntarily conveyed numerical information . . . [and] assumed the risk that the company would reveal to police the numbers he dialed."); United States v. Miller, 425 U.S. 435, 443 (1976) (holding that a bank depositor "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government . . . even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed").

15. *E.g.*, 18 U.S.C. § 2703(d) (2012); *see also infra* text accompanying notes 51-54 (detailing subpoena law).

I. The Interaction of Cause and Object Justifications

Probable cause is the central justificatory concept in Fourth Amendment jurisprudence. As defined by the Supreme Court in the recent decision of *Safford Unified School District #1 v. Redding*,[16] probable cause to search exists when the known facts "raise a 'fair probability,' or a 'substantial chance,' of discovering evidence of criminal activity."[17] Probable cause is not "hypertechnical"[18] but rather consists of a "flexible, common sense standard."[19] As this language suggests, and as many admit, probable cause is a slippery concept.[20] But there is at least general agreement that, conceived of as a standard of proof, it falls somewhere below both the no-reasonable-doubt standard and the clear and convincing evidence standard, somewhat above reasonable suspicion, and in the general vicinity of, albeit somewhat below, the preponderance of the evidence standard used in civil courts.[21] The Court has resisted quantification of these standards but, as a useful heuristic, reasonable doubt might be equated with a 90% to 95% probability,[22] clear and convincing evidence with a 75% probability,[23] preponderance with a 51% probability,[24] probable cause between a 40% to 50% chance that the search will be successful,[25] and reasonable suspicion somewhere below that.[26] In fact, one survey asking over 160 federal judges to assign percentages to the latter two concepts found that their answers averaged out to 48% for probable cause[27] and 31% for reasonable

16. 557 U.S. 364 (2009).

17. *Id.* at 371.

18. Illinois v. Gates, 462 U.S. 213, 236 (1983) (citing United States v. Ventrusca, 380 U.S. 102, 109 (1965)).

19. *Id.* at 239.

20. *See, e.g.*, Erica Goldberg, *Getting Beyond Intuition in the Probable Cause Inquiry*, 17 LEWIS & CLARK L. REV. 789, 801 (2013) ("Judges, scholars, and practitioners hold varying views as to the burden imposed by probable cause, with the largest number of judges clustering in the range between 30% and 60%.").

21. *See supra* note 8 and accompanying text; *cf. Gates*, 462 U.S. at 235 ("Finely tuned standards such as proof beyond a reasonable doubt or by a preponderance of the evidence, useful in formal trials, have no place in the magistrate's decision.").

22. *See* C.M.A. McCauliff, *Burdens of Proof: Degrees of Belief, Quanta of Evidence, or Constitutional Guarantees?*, 35 VAND. L. REV. 1293, 1325 tbl.2 (1982).

23. *Id.* at 1328 tbl.5.

24. *Id.* at 1331 tbl.7.

25. *Id.* at 1327 tbl.3.

26. *Id.* at 1328 tbl.4.

27. *Id.* at 1327 tbl.3.

suspicion.[28] Probable cause and reasonable suspicion will never be defined precisely, but courts have become used to the concepts.

Modern courts pay much less attention, however, to what this essay is calling the "object" of the probable cause and reasonable suspicion requirements. Note, for instance, that *Redding*'s definition of probable cause speaks of a fair probability of "discovering *evidence of criminal activity*,"[29] without further elaboration or caveat. Yet many of the Supreme Court's Fourth Amendment cases have both analyzed and approved searches for evidence of noncriminal wrongdoing.[30] Thus *Redding*'s use of the word "criminal" must be taken with a grain of salt, a fact that is worth emphasizing. That government officials can invade our "houses, persons, papers and effects"[31] looking for proof of mere regulatory infractions raises large and difficult issues that are worthy of article-length treatment on their own.[32]

This essay will instead confine itself to analysis of criminal cases and their close brethren, national security cases. Even with this narrowed focus, other ambiguities arise. Classic examples of criminal evidence include fruits of a crime (such as money stolen from a bank), instrumentalities of crime (such as a murder weapon), and contraband (such as illicit drugs). But the courts have authorized searches for and seizures of many other types of items in criminal cases. First, courts have issued warrants based on probable cause to believe that police will be able to find what used to be called "mere evidence,"[33] such as negatives in the possession of a third party that might help prove a crime occurred,[34] an invoice from an attorney who is alleged to be a co-conspirator,[35] or company logs proving that a

---

28. *Id.* at 1328 tbl.4.

29. Safford Unified Sch. Dist. #1 v. Redding, 557 U.S. 364, 371 (2009) (emphasis added).

30. *See, e.g.*, Wyman v. James, 400 U.S. 309, 318-19 (1971) (permitting the government to condition receipt of welfare benefits on warrantless searches of residences); Camara v. Municipal Ct. of City & Cnty. of S.F., 387 U.S. 523, 538-39 (1967) (permitting searches of residences to enforce health and safety codes after a warrant has been obtained).

31. U.S. CONST. amend. IV.

32. I develop some preliminary ideas on this topic in Christopher Slobogin, *Government Dragnets*, LAW & CONTEMP. PROBS., Summer 2010, at 107; *see also* Eve Brensike Primus, *Disentangling Administrative Searches*, 111 COLUM. L. REV. 254 (2011).

33. *See* Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 309-10 (1967).

34. *See* Zurcher v. Stanford Daily, 436 U.S. 547, 567-68 (1978) (holding that a warrant is sufficient to obtain negatives from a newspaper office).

35. Gouled v. United States, 255 U.S. 298, 310 (1921) (holding that seizure of an attorney's bill for legal services was impermissible), *abrogated by Hayden*, 387 U.S. 294.

person has phoned the number of a victim.[36] Further, the "mere" evidence sought may be highly circumstantial, or very tangential to any element in the case, such as items proving gang membership in a case of domestic violence,[37] or indicia of house ownership in a case involving possession or sale of drugs found in a residence already known to be occupied by the suspect.[38] Finally, if the word "evidence" is read broadly to include information that would not be considered relevant in court but might help catch the perpetrator of criminal activity, then the object of the search could also include information that can help locate the individual, such as her cell phone signals or credit card purchases.[39]

With the exception of the locational examples, these various gradations of "evidence" have not given pause to courts construing the Fourth Amendment, at least since the Supreme Court's 1967 decision in *Warden, Maryland Penitentiary v. Hayden*, which eliminated the prohibition on seizure of mere evidence.[40] Over four decades earlier, in *Gouled v. United States*, the Court had held that search warrants "may not be used as a means of gaining access to a man's house or office and papers solely for the purpose of making search to secure evidence to be used against him in a criminal or penal proceeding" unless the government has a superior property interest in the evidence, as is the case with fruits and instrumentalities of crime and contraband.[41] In *Hayden*, however, the Court reversed this aspect of *Gouled*, stating:

> Privacy is disturbed no more by a search directed to a purely evidentiary object than it is by a search directed to an

---

36. Smith v. Maryland, 442 U.S. 735, 745 (1979) (holding that police could seize a phone record showing the defendant phoned the victim).

37. Messerschmidt v. Millender, 132 S. Ct. 1235, 1248-49 (2012) (implying that a warrant can authorize a search for evidence of gang membership on these facts). *Millender* is discussed further in the text accompanying notes 81-93. *See also* United States v. Rubio, 727 F.2d 786, 792 (9th Cir. 1983) (holding that "a narrowly drawn, and properly issued and executed warrant which authorizes the search for indicia of membership or association" does not violate the First Amendment).

38. United States v. McLaughlin, 851 F.2d 283, 286 (9th Cir. 1988) (holding that "[a] search warrant may be used, not only to gather evidence of a criminal activity, but also to gather evidence of who controlled the premises suspected of connection with criminal acts").

39. *E.g.*, *In re* Application of United States for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Telephone, 849 F. Supp. 2d 526, 536 (D. Md. 2011) (holding that a warrant may not authorize seizure of data about a suspect's location unless he is a fugitive because otherwise the data are not evidence).

40. 387 U.S. 294, 302 (1967).

41. 255 U.S. 298, 309 (1921).

> instrumentality, fruit, or contraband. A magistrate can intervene in both situations, and the requirements of probable cause and specificity can be preserved intact. Moreover, nothing in the nature of property seized as evidence renders it more private than property seized, for example, as an instrumentality; quite the opposite may be true. Indeed, the distinction is wholly irrational, since, depending on the circumstances, the same 'papers and effects' may be 'mere evidence' in one case and 'instrumentality' in another.[42]

Hayden reserved for another day the issue of whether mere evidence that is "testimonial" in nature—such as documents—may be seized, suggesting that the Fifth Amendment's prohibition against compelling testimony could limit its holding in some situations.[43] But later cases made clear that a search for papers does not implicate the Fifth Amendment, because neither the content of the papers nor their production is compelled by the State.[44] Subsequent cases also held that even papers that could be said to be protected by the First Amendment may be seized upon the usual, probable cause showing required for searches of other types of items.[45] In short, the Constitution permits searches for and seizures of any "things"—to use the Fourth Amendment's language—regardless of their nature, so long as there is adequate cause to believe they will be found and they have some nexus to suspected wrongdoing.[46]

---

42. *Hayden*, 387 U.S. at 302.

43. *Id.* at 302-03 ("The items of clothing involved in this case are not 'testimonial' or 'communicative' in nature, and their introduction therefore did not compel respondent to become a witness against himself in violation of the Fifth Amendment.").

44. *See, e.g.*, Andresen v. Maryland, 427 U.S. 463, 473-74 (1976) ("[A]lthough the Fifth Amendment may protect an individual from complying with a subpoena for the production of his personal records in his possession because the very act of production may constitute a compulsory authentication of incriminating information, a seizure of the same materials by law enforcement officers differs in a crucial respect—the individual against whom the search is directed is not required to aid in the discovery, production, or authentication of incriminating evidence." (internal citations omitted)).

45. New York v. P. J. Video, Inc., 475 U.S. 868, 875 (1986) ("[A]n application for a warrant authorizing the seizure of materials presumptively protected by the First Amendment should be evaluated under the same standard of probable cause used to review warrant applications generally.").

46. For an argument that the Court's jurisprudence in this area is wrongheaded, see Note, *Formalism, Legal Realism, and Constitutionally Protected Privacy Under the Fourth and Fifth Amendments*, 90 HARV. L. REV. 945, 987-88 (1977).

Yet, as a general rule, the further one moves from the classic triad of fruits of crime, instrumentalities of crime, and contraband, the greater the government's authority to invade privacy becomes. As Judge Learned Hand stated,

> If the search is permitted at all, perhaps it does not make so much difference what is taken away, since the officers will ordinarily not be interested in what does not incriminate, and there can be no sound policy in protecting what does. Nevertheless, limitations upon the fruit to be gathered tend to limit the quest itself . . . .[47]

Consider, for instance, some of the examples of mere evidence given earlier. Gang insignia could be anywhere in the home. Searches for indicia of ownership can range far beyond a search for weapons or contraband, to include, in the words of the boilerplate warrant language often used in one jurisdiction, "all papers, documents, and effects which tend to show possession, dominion and control over said premises, including fingerprints, handwritings, clothing and objects bearing a form of identification such as a person's name, photograph, Social Security number or driver's license number."[48] Most relevant to this essay, information about location, associations, and activities around the time of a crime might be found in a wide range of records, buried in the middle of reams of information that have nothing to do with the suspected criminal activity.[49]

Furthermore, in the absence of a mere evidence limitation, searches are permissible even if the *sole* goal is obtaining such attenuated evidence. As

---

47. United States v. Poller, 43 F.2d 911, 914 (2d Cir. 1930); *see also* United States v. A Parcel of Land, Bldgs., Appurtenances, & Improvements, Known as 92 Buena Vista Ave., Rumson, N.J., 507 U.S. 111, 121 (1993) (citing Zurcher v. Stanford Daily, 436 U.S. 547, 577-80 (1978) (Stevens, J., dissenting)) ("The holding in [*Hayden's holding*] that the Fourth Amendment did not prohibit the seizure of 'mere evidence' marked an important expansion of governmental power.").

48. Laurence A. Benner & Charles T. Samarkos, *Searching for Narcotics in San Diego: Preliminary Findings from the San Diego Search Warrant Project*, 36 CAL. W. L. REV. 221, 254 (2000).

49. Note that the same issue arises when the police are validly intruding into a particular area or document looking for evidence of one crime and come across an item in plain view that might be evidence of another wrongdoing. *See* Texas v. Brown, 460 U.S. 730, 738 (1983) ("The seizure of property in plain view involves no invasion of privacy and is presumptively reasonable, assuming that there is probable cause to associate the property with criminal activity."). Again, however, nothing in the plain view doctrine limits what the evidence can be. See *id.* at 737 (stating that the seized item need only be "evidence of a crime, contraband or otherwise subject to seizure")).

one commentator noted shortly after *Hayden* was decided, without some limit on the object of a search an imaginative officer could emasculate the probable cause requirement even in connection with private documents:

> According to the language of the [*Hayden*] majority, if the object seized will aid in the apprehension, conviction, or identification of the accused it may be seized. . . . Certainly all private letters and papers would aid in identifying the handwriting of the accused. The diary of an accused might be helpful in destroying his alibi. The private files of a suspect might be useful in his apprehension. Surely an 'unpatriotic' political sentiment expressed in private writings would aid in the conviction of one accused of sabotage or espionage.[50]

The distinction between the standard of proof and the object of the search also arises in connection with the law of subpoenas. In *United States v. R. Enterprises, Inc.*,[51] the Supreme Court pointed out that the typical discovery subpoena, issued after a complaint or charge is filed, will only issue if it is based on "a reasonably specific request for information that would be both relevant and admissible at trial."[52] In contrast, a grand jury subpoena, issued during the investigative phase before a charge has been filed, should only be denied when "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation."[53] In both cases, "relevance" is the standard of proof. But the object of the subpoena in the two situations is quite different. In the discovery context, the object is an item or items considered relevant to a particular charge, whereas in the investigative context it is anything relevant to the "general subject" of an investigation, which does not have to be aimed at any particular charge or person. As the Court acknowledged, the latter standard is much easier to meet than the former.[54]

In short, defining concepts like probable cause, reasonable suspicion, and like standards of proof is only half the job of delineating justificatory

---

50. Fournier J. Gale, Comment, *Constitutional Law-Evidence-Clothing of Suspect Held Admissible Even Though It Was "Mere Evidence" of Crime*, 20 ALA. L. REV. 149, 157 (1967).

51. 498 U.S. 292 (1991).

52. *Id.* at 299 (citing United States v. Nixon, 418 U.S. 683, 700 (1974)).

53. *Id.* at 301.

54. *Id.* at 298-99 (explaining why grand jury subpoenas need not meet the requirements imposed on discovery).

standards. Some attention should also be paid to the extent to which the items that law enforcement believes the search will uncover can further an investigation. The object of the search might be "mere evidence" or not evidence at all; it might be aimed at helping prove a specific crime or it might be information about a crime as-yet unknown or even not yet committed. Defining the object of a search can be as important as defining the level of certainty that the object will be found.

II. The LEATPR Standards and the NSA's Metadata Program

The American Bar Association's Criminal Justice Standards on Law Enforcement Access to Third Party Records, adopted by the ABA House of Delegates in February 2012,[55] vary both the standard of proof and the object of the search in their provisions defining the justification necessary to obtain information from third party records. The Standards recognize three species of courts orders: the first based on "probable cause to believe the information in the record contains or will lead to evidence of crime," the second on "reasonable suspicion to believe the information in the record contains or will lead to evidence of crime," and the third on a finding that the "record is relevant to an investigation."[56] The Standards also provide for a "prosecutorial certification" to a judge that must meet the relevance-to-an-investigation test, and for a subpoena from a prosecutor or agency that may be issued on the same ground.[57] Finally, the Standards describe a standard, called an "official certification," that requires a "reasonable possibility that the record is relevant to initiating or pursuing an investigation."[58] That these phrases are meant to reflect decreasingly demanding levels of justification is made clear by subsequent provisions that require a probable cause court order for "highly protected" information and a reasonable suspicion court order (or, in the alternative, a relevance determination by a judge or prosecutor) for "moderately protected information."[59] Further, only a subpoena meeting the relevance standard is needed for "minimally protected information,"[60] and an official certification meeting the "reasonable possibility" standard suffices for accessing "de-

55. CRIMINAL JUSTICE STANDARDS ON LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS iii (2013).

56. STANDARD 25-5.2(a)(i)-(iii).

57. STANDARD 25-5.2(a)(iv), (b).

58. STANDARD 25-5.2(c).

59. STANDARD 25-5.3(a)(i)-(iii).

60. STANDARD 25-5.3(a)(iii).

identified" records (i.e., records that are not easily linked to an identified person).[61]

In general, the idea that the level of justification should become less onerous as the privacy content of the sought-after records decreases makes sense. I have defended and elaborated on this proportionality idea elsewhere and am gratified that the ABA has endorsed it.[62] Although parsing the differences between probable cause and the Standards' other standards of proof can be difficult, most would probably agree that relevance is an easier standard to meet than either probable cause or reasonable suspicion.[63] One could also conclude that relevance as determined by a judge is different, and more restrictive, than relevance certified by a prosecutor and rubberstamped by a judge, which in turn is more restrictive than relevance determined by a prosecutor or an administrative bureaucrat who does not have to go to a judge at all.[64] So at least the Standards could be said to create a hierarchy that makes conceptual sense.

More important to the focus of this essay is the fact that only the probable cause and reasonable suspicion standards are linked with the phrase "evidence of crime." The other standards merely require a connection "to an investigation." Thus, the various relevance provisions in the LEATPR Standards are more relaxed than traditional Fourth Amendment justifications in *two* ways—not just in terms of the standard of proof but in terms of the object of the surveillance.

Consider in light of this discussion the NSA's bulk collection of metadata—again, the recently controversial program that is aimed at accumulating, anonymously as an initial matter, the phone and text transmittal information of everyone in the country. This information is clearly not contraband or fruits of crime, and only a very stretched definition of the word "instrumentality" would place a phone number or email address in this third category, even if it were a number used by a criminal to carry out a crime. The metadata might be considered "mere

---

61. STANDARD 25-5.6(a).

62. *See* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 21-47 (2007).

63. *Cf. id.* at 38-39 (proposing "four tiers" of justification: relevance, reasonable suspicion, probable cause, and clear and convincing evidence).

64. *Cf.* RICHARD VAN DUIZEND, L. PAUL SUTTON & CHARLOTTE A. CARTER, THE SEARCH WARRANT PROCESS: PRECONCEPTIONS, PERCEPTIONS, AND PRACTICES 148-49 (1985) (finding that requiring police to make a showing of probable cause to a judge increased the standard of care).

evidence" if, for instance, it could help the government discover that certain people are communicating with a known terrorist. But at the time of the bulk collection, those links would not be known; the NSA would subsequently have to query the data to learn about those links. Thus, one would be hard pressed to say that, at the time of the bulk collection, the government meets the relevance standard, much less the probable cause or reasonable suspicion standards, if the object of the seizure is *Redding's* "evidence of criminal activity" or the LEATPR Standards' "evidence of crime" that is associated with the probable cause and reasonable suspicion standards.

On the other hand, the bulk data might be relevant "to an investigation," and there is certainly a reasonable possibility that the data will be relevant "to initiating or pursuing an investigation" (the two phrases describing the object of the search in the Standards' other justification provisions).[65] That is in fact what the government successfully argued in front of the Foreign Intelligence Surveillance Court (FISC) under section 215 of the Patriot Act, which permits authorization of "any tangible things (including books, records, papers, documents, and other items)" that are "relevant to an authorized investigation . . . [designed] to protect against international terrorism or clandestine intelligence activities."[66] According to a 2009 opinion from the FISC, "The government depends on this bulk collection because if production of the information were to wait until the specific identifier connected to an international terrorist group were determined, most of the historical connections (the entire purpose of this authorization) would be lost."[67] The court continued,

> Because the subset of terrorist communications is ultimately contained within the whole of the metadata produced, but can only be found after the production is aggregated and then queried using identifiers determined to be associated with identified international terrorist organizations, the whole production is *relevant to the ongoing investigation* out of necessity.[68]

---

65. STANDARD 25-5.2(a)(iii), (c).

66. The USA PATRIOT Act § 215, 50 U.S.C §§ 1861 (a)(1), (b)(2)(A) (2012).

67. *In re* Application of the F.B.I. for an Order Requiring the Prod. of Tangible Things From . . . , BR 13-109, 22, (Foreign Intelligence Surveillance Ct. July 29, 2013), *available at* https://www.documentcloud.org/documents/791759-br13-09-primary-order.html.

68. *Id.* (emphasis added).

The LEATPR Standards appear to endorse precisely the same argument. Standard 25-5.6 permits access to "de-identified records" if there is a "reasonable possibility that [a] record [will be] relevant [to] . . . an investigation."[69] De-identified records are defined as records that are not "linked" or are not "linkable through reasonable efforts" to an identifiable person, which arguably describes the status of the anonymous numbers acquired during the bulk collection.[70]

Now consider how the Standards would deal with the NSA's process of querying the records obtained through the bulk collection process (with apologies in advance for the complicated textual analysis). For this process of linking the records to a particular person, the Standards require greater justification, which varies depending on the nature of the record. Under Standard 25-5.3(a), if phone metadata is considered "moderately protected," for instance, it can be linked to a particular person only if, under the ABA's preferred standard for those types of records, a court finds "reasonable suspicion . . . the information in the record contains or will lead to evidence of crime."[71] The Standards' two-step process—incorporating the distinction between the standard for acquiring anonymous records, which is relatively easily met, and the standard for investigating identified records, which imposes a stronger justification—is known as "selective revelation," and has been endorsed by a number of commentators.[72]

At least at its initial stage, the NSA's procedure for querying the de-identified metadata it has collected in bulk appears to meet or exceed the selective revelation requirements imposed by the Standards. According to the NSA, analysis of the metadata it has collected begins with what the NSA calls a "seed identifier," such as a phone number that the agency (double-checked by the FISC) has "reasonable, articulable suspicion" to believe is associated with a terrorist organization.[73] That standard is similar

---

69. STANDARD 25-5.2(c), 25-5.6(a) (requiring an "official certification" to obtain de-identified records).

70. STANDARD 25-1.1(g). *But see* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010) (explaining that de-anonymization is very easily carried out).

71. STANDARD 25-5.2(a)(ii), 25-5.3(a)(ii).

72. *See generally* K. A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 1, 79-80 (2003) (describing selective revelation).

73. NAT'L SEC. AGENCY, THE NATIONAL SECURITY AGENCY: MISSIONS, AUTHORITIES, OVERSIGHT AND PARTNERSHIPS 5 (2013), *available at* http://www.nsa.gov/publicinfo/files/speeches_testimonies/2013_08_09_the_nsa_story.pdf. Until January, 2014, this determination was made by NSA analysts; the FISC was only involved in approving the list

to the Standards' preferred standard of proof for obtaining moderately protected records (assuming the word "crime" is read to include terrorist acts and analogous acts).[74]

But the NSA does not stop there. While the agency has not explicitly stated how many links beyond the seed identifier it investigates, testimony by an NSA official in the summer of 2013 indicated that the FISC has allowed NSA staffers to "go out two or three hops" from the target.[75] In other words, the NSA attempts to identify everyone who communicates with the seed identifier, as well as those who communicate with the first and second links to that identifier. Given the suspected terrorist affiliation of the seed identifier, the Standards' reasonable suspicion standard might be met with respect to the first link. But it would be hard to conclude that, in the absence of any other information, the government has reasonable suspicion that the identity of a person three links out from the seed identifier is "evidence of crime" or could "lead to" such evidence. This type of concern is presumably what motivated President Barack Obama, in January 2014, to declare that henceforth the NSA would only be permitted to query two hops from the seed identifier.[76]

---

of terrorist organizations, not in confirming that reasonable suspicion existed in connection with a seed identifier. *Id.* On January 17, 2014, President Obama apparently ordered that, in non-emergency situations, the FISC must sign off on the NSA's reasonable suspicion determination. *Obama's Speech on N.S.A.'s Phone Surveillance*, N.Y. TIMES, Jan. 17, 2014, *available at* http://www.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html?_r=0 ("I have directed the Attorney General to work with the Foreign Intelligence Surveillance Court so that during this transition period, the database can be queried only after a judicial finding or in the case of a true emergency."). Legislation proposed by the Obama Administration in March, 2014, would codify this rule. *See* Charlie Savage, *Obama to Call for End to N.S.A's Bulk Data Collection*, N. Y. TIMES, March 24, 2014.

74. Note also that, under the Standards, if a justification requirement "would render law enforcement unable to solve or prevent an unacceptable amount of otherwise solvable or preventable crime . . . a legislature may consider reducing . . . the level of protection for that type of information." STANDARD 25-4.2(b). Given the already minimal justification requirements for most records, this concession to law enforcement seems unnecessary and, in any event, illegitimately states that if a justification standard gets in the way of law enforcement, law enforcement agencies can disregard it.

75. Kris, *supra* note 3, at 12 n.49 (quoting *The Administration's Use of FISA Authorities: Hearing Before the H. Comm. on the Judiciary*, 113th Cong. (2013) (statement of John C. Inglis, Deputy Director, NSA)).

76. *Obama's Speech*, *supra* note 73 ("Effective immediately, we will only pursue phone calls that are two steps removed from a number associated with a terrorist organization instead of the current three.").

Recall, however, that the Standards recognize an alternative justification for cases involving moderately protected records. If that alternative standard is applied, the government would only need to obtain "a judicial determination that the record is relevant to an investigation" or to produce a "prosecutorial certification that the record is relevant to an investigation."[77] Not only is relevance a lower standard of proof than reasonable suspicion, the object of the search—an "investigation"—is much more capacious. Analogous to the distinction made by the Court in *R. Enterprises*, whereas the phrase "leading to evidence of crime" suggests that some specific wrongdoing (in this context, association with a terrorist) is the object of the search,[78] the word "investigation" implies an exploration of anyone who might be connected to a seed identifier, which imposes virtually no limits on the government's query.[79] Perhaps the Standards' recognition of an even lower standard—the aforementioned provision regarding de-identified records that requires only a "reasonable possibility that the record is relevant to *initiating or pursuing* an investigation"—can be said to cabin the phrase "relevant to . . . an investigation"[80] in the Standards' other provisions. But the fact remains that much may ride on which of the alternative standards in Standard 25-5.3(a)(ii) the jurisdiction adopts. The combination of the lower standard of proof ("relevance" compared to "reasonable suspicion") and the more indistinct object of the surveillance ("an investigation" compared to "evidence of crime") markedly reduces the government's burden.

Indeed, one could easily make the argument that even the identity of a person ten "hops" from the seed identifier is "relevant to an investigation," if the word "investigation" encompasses not just attempts to get information about the seed identifier and his known associates but also about "terrorists" or "threats to national security." In contrast, the government's argument would be much harder if it had to show that the identity of a given link is relevant in the sense that it could "lead to *evidence*" of a specific threat to national security; that language implies that the name identified via the query must either be evidence or connect directly to such evidence. Application of the Standards to the NSA's metadata program illustrates that defining the object of the search is at least as important as defining the level of certainty the decision maker must have that the object will be discovered.

---

77. STANDARD 25-5.2(a)(iii)-(iv), 25.3(a)(ii).

78. *See supra* text accompanying notes 51-54.

79. The commentary to the Standards does not discuss this issue.

80. STANDARD 25-5.2(c) (emphasis added).

III. Defining the Object of the Search

So how should the object of a search be defined? The seeds of an answer are found in the recent Supreme Court decision in *Messerschmidt v. Millender*,[81] the case involving evidence of gang membership that was briefly alluded to above. In *Millender*, the police obtained a search warrant to search the home of the Millenders, believing that one Jerry Bowen lived there and that they might find evidence that would help prove he had assaulted his ex-girlfriend.[82] Because the ex-girlfriend said Bowen was a gang member, among the items listed in the warrant were "[a]rticles of evidence showing . . . affiliation with any [s]treet [g]ang."[83]

Millender challenged the validity of this aspect of the warrant with the argument that, because membership in a gang is not a crime, a magistrate should not be authorized to issue a warrant aimed merely at obtaining evidence of gang membership.[84] Because the officer who drafted the warrant application admitted that the crime being investigated was not gang-related but rather was a domestic dispute,[85] and because the facts supported that assumption,[86] Millender contended that the gang information was irrelevant to criminal prosecution.

But the majority in *Millender* strongly signaled that it felt otherwise.[87] First, it stated that evidence of gang membership could have shown that the assault was not motivated, as the ex-girlfriend had suggested, by "the souring of [a] romantic relationship," but rather by a fear that the victim

---

81. 132 S. Ct. 1235 (2012).

82. *Id.* at 1242.

83. *Id.*

84. *Id.* at 1247 (noting that Millender contended that "'the magistrate [could not] have reasonably concluded, based on the affidavit, that Bowen's gang membership had anything to do with the crime under investigation' because '[t]he affidavit described a 'spousal assault' that ensued after Kelly decided to end her 'on going dating relationship' with Bowen' and '[n]othing in that description suggests that the crime was gang-related'"); *see also id.* at 1257 n.7 (Sotomayor, J., dissenting) (noting that membership in a gang is not a crime in the state of California).

85. *Id.* at 1248 n.6.

86. *Cf. id.* at 1255 (Sotomayor, J., dissenting) ("Every piece of information . . . accorded with Detective Messerschmidt's conclusion: The crime was domestic violence that was not gang related.").

87. Since the issue in *Millender* was whether the officer had qualified immunity, the Court's discussion focused on whether a "reasonable officer" could have believed the gang insignia would be evidence of crime, not whether the Fourth Amendment authorizes search of such items on the facts of *Millender*. *Id.* at 1244.

would disclose Bowen's gang activity to the police.[88] Second, based on the same reasoning, the evidence might have supported obstruction of justice charges.[89] The majority also speculated that the evidence could have been used to impeach Bowen if he had taken the stand and testified that he didn't use a gun during the assault; the evidence of gang membership could have shown he was familiar with guns and the kind of gun the victim said he used.[90] As the dissenting opinions on this issue pointed out, the majority had to be very imaginative in coming up with these possible uses of items showing Bowen was associated with a gang.[91] Even so, the majority was right to surmise that the gang insignia, had it been found (in fact, it was not[92]), *could* have helped prove motive or *could* have helped impeach.

Note that the issue in *Millender* was not whether the standard of proof was met. Given the victim's statements, the police clearly had probable cause to believe they would find gang-related items in the Millender's house. Rather, the issue in *Millender* was the relevance of the object of the search—whether the items identified in the warrant could be useful in a subsequent criminal prosecution.

While the majority in *Millender* had no difficulty answering this question in the affirmative, the precedent it relied on—in particular, *Warden, Maryland Penitentiary v. Hayden*—appears to require a different answer, an answer that is very helpful in thinking about the object of the search issue. In bolstering its conclusion that the gang information in *Millender* could be seized, the Court stated that "[t]he Fourth Amendment does not require probable cause to believe evidence will conclusively establish a fact before permitting a search, but only 'probable cause . . . to believe the evidence sought *will aid* in a particular apprehension or conviction.'"[93] The Court seemed to think *Hayden*'s language, particularly the use of the word "aid," supported its case. But look closely at the quoted language. *Hayden* says that the object of the search must be evidence that "*will* aid"

88. *Id.* at 1247.

89. *Id.* at 1248.

90. *Id.*

91. *Id.* at 1251 (Kagan, J., concurring in part and dissenting in part) (referring to "the Court's elaborate theory-spinning"); *id.* at 1254 (Sotomayor, J., dissenting) ("The Court reaches this result only by way of an unprecedented, *post hoc* reconstruction of the crime that wholly ignores the police's own conclusions, as well as the undisputed facts presented to the District Court.").

92. *Id.* at 1243 (noting that the search resulted only in the seizure of a weapon and ammunition).

93. *Id.* at 1257 n.7 (emphasis omitted) (quoting Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 307 (1967)).

apprehension or conviction, not "might aid." If probable cause (the standard of proof at issue in *Millender*) is quantified at 40-50%, then *Hayden*'s language as applied to *Millender* requires a 40-50% likelihood that the gang information *will* aid in apprehension or conviction. Despite the majority's innovative hypotheses about how the evidence could have been used, that showing is not possible on the facts of *Millender*. Only if the victim had said, or the police had other plausible reasons to believe, that Bowen was trying to hurt her to shut her up about his gang activities would such grounds exist.

Now consider a case involving access to third party records. Assume police have a tip from a reliable informant that John Doe is a methamphetamine dealer. Can they now access Doe's bank records for the past year to see if he has made large deposits from time to time, or his phone records over the next several months to see if he is calling known drug consumers, or his credit card records for the past two weeks to see if he is buying certain types of materials? Whether it is interpreting the Fourth Amendment or statutory language, the Supreme Court's *Millender* majority might say yes, because any of this information—all of which can be particularly described sufficiently for Fourth Amendment purposes—*might* aid in Doe's prosecution. But if the standard of proof were probable cause or reasonable suspicion, and *Hayden*'s definition of the object of the search is adopted, a good argument can be made that access to these records should not be allowed, at least if the informant has only told us that Doe is selling drugs. In that case, there is only a small chance that any given set of records will aid in Doe's conviction. Even if large deposits, calls to particular people, or purchases of certain items were discovered, that information is at least as consistent with legal activity as illegal activity. Only if the informant provides a particular date Doe sold drugs or provided other more particularized information about what might be in the records would there be a plausible argument that any given bank, phone, and credit card records *will* aid the prosecution's case.

Notably, in their definition of probable cause and reasonable suspicion, the ABA Standards adhere to *Hayden*'s language. Both definitions speak in terms of whether a records search *will* obtain evidence of crime or lead to such evidence.[94] That formulation endorses a relatively tight approach to the object of the search. In contrast, as noted above, the Standards' definition of relevance adopts a much more capacious approach to the

94. *Compare* STANDARD 25-5.2(a)(i)-(ii), *with Hayden*, 387 U.S. at 307.

object of the search by referring merely to "an investigation" of criminal activity.[95]

I have proposed a regime for accessing third party records that differs from the ABA Standards (and the Court's apparent position after *Millender*) in several ways, two of which are directly relevant to this discussion.[96] First, because it potentially imposes no meaningful limitation on law enforcement, I avoid the relevance standard of proof and propose that the government should have to demonstrate either probable cause or reasonable suspicion when it is seeking access to records held by an institutional third party in connection with an investigation of an individual.[97] More important, for present purposes, is the way in which my proposal defines the object of the search in connection with these two standards of proof. The proposed definition of probable cause is as follows: "[a]n articulable belief that a search will more likely than not produce contraband, fruit of crime, or other significant evidence of wrongdoing."[98] And the proposed definition of reasonable suspicion is: "An articulable belief that a search will more likely than not lead to evidence of wrongdoing."[99]

Note that both definitions adopt a "more likely than not," or preponderance of the evidence, standard of proof. There is no attempt to differentiate between the two standards based on the level of certainty (for instance, by conceptualizing probable cause as "more likely than not" and reasonable suspicion as something below that). Rather, the difference between the standards lies entirely in the object of the search. The probable

---

95. *See* STANDARD 25-5.2(a)(iii)-(iv).

96. 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 (2012). Another difference between the proposal and the Standards that is indirectly relevant to this discussion is the way the proposal defines the hierarchy of records. Specifically, I proposed that probable cause be required if the records described activities over more than a forty-eight-hour period, and that the reasonable suspicion standard should apply in all other situations in which protected records are accessed. *Id.* at 28. I argued that this temporally defined method of differentiating the justification required for a records search, while somewhat arbitrary, is more easily applied than the ABA's multifactor test in Standard § 25-4.1, *id.* at 28-29, and is also more consistent with the concurring opinions in *United States v. Jones*. *See* 132 S. Ct. 945, 964 (Alito, J., concurring) ("[T]he use of *longer term* GPS monitoring in investigations of most offenses impinges on expectations of privacy." (emphasis added)); *see also id.* at 955 (Sotomayor, J., concurring) (agreeing with Justice Alito's statement).

97. Slobogin, *supra* note 96, at 28 (requiring either probable cause or reasonable suspicion for "targeted data searches").

98. *Id.* at 20.

99. *Id.* at 22.

cause standard requires that the object be contraband, fruits of crime, or other significant evidence of wrongdoing. The last phrase is obviously somewhat vague, but is meant to be informed by its association with contraband and fruits of crime. In other words, searches for mere evidence, highly circumstantial or tangible evidence, or information that is not evidence at all (such as the location of a suspect), are not authorized in those situations that require probable cause. In contrast, reasonable suspicion merely requires a belief that, more likely than not, the search will "lead" to evidence of wrongdoing, and thus could contemplate accessing records that are not significant evidence of crime.[100] If these definitions of probable cause and reasonable suspicion replaced the Standards' justificatory standards (but the Standards' regulatory structure were otherwise retained), they would require the government to show that accessing "highly protected records" would more likely than not produce significant evidence of crime, and that accessing other types of records (at least other than those that are denominated "unprotected") would require a showing that the information they contained would more likely than not lead to any evidence of wrongdoing.

With these proposed adjustments to the Standards in mind, return to the NSA's metadata program. Assuming the NSA queries were aimed at moderately protected records, they could only proceed under the adjusted Standards if they would likely lead to evidence of wrongdoing. This threshold would become progressively harder to meet with each link beyond the original target. It would probably permit identification of the first link from the seed identifier,[101] but might well prohibit any further linking, barring additional articulable information about the seed identifier or the first link that made pursuit of numbers further down the chain reasonable. In short, the definition of the search's object could place a significant limitation on the NSA's metadata program.[102]

---

100. Thus, for instance, the reasonable suspicion standard would not bar obtaining location information about a suspect, since that information could lead to evidence of crime. *See id.*

101. As the Supreme Court stated in *CIA v. Sims*, "[B]its and pieces of data 'may aid in piecing together bits of other information even when the individual piece is not of obvious importance in itself.'" 471 U.S. 159, 178 (1985) (quoting Halperin v. CIA, 629 F.2d 144, 150 (D.C. Cir. 1980)).

102. The probable cause and reasonable suspicion standards I propose only apply to "targeted" searches, and thus would not govern the NSA's initial, bulk collection process, which is aimed at the population at large. A separate aspect of the proposed regulatory scheme would permit these types of "general searches" only if "authorized by legislation or regulations issued pursuant to such legislation" and only if they applied evenly to those

Conclusion

In fashioning rules governing access to records or any other type of search activity, courts and legislatures should be alert not only to standards of proof, such as probable cause or reasonable suspicion, but also to the object of the search. While the Fourth Amendment apparently puts no restrictions on the types of information that the government may gather so long as it has a nexus to wrongdoing, however attenuated, a failure to place further restrictions on the object of a search can vastly increase the government's authority to intrude into privacy. The ABA Standards on Law Enforcement Access to Third Party Records recognize this point and to a small extent differentiate government authority to act based on it. But as illustrated by this essay's analysis of how the Standards would apply to the NSA's metadata surveillance program, the ABA's provisions could authorize virtually unlimited access to all but the most highly protected records. A regime that limited the object of the search to significant evidence of wrongdoing when probable cause is required and to information that will lead to such evidence when reasonable suspicion is required would provide a more meaningful and coherent restriction on government access to third party records.

---

affected. *See* Slobogin, *supra* note 96, at 30-32 (describing regulation of "general public and data searches"). This formulation is an implementation of political process theory, and would probably permit bulk data collection, given the passage and repeated reaffirmation of section 215 (despite Snowden's revelations) and given its application to the entire country rather than a discrete group. *See* Christopher Slobogin, *Panvasive Surveillance, Political Process Theory and the Nondelegation Doctrine*, 102 GEO. L.J. (forthcoming 2014). If, however, the legislation authorizing the bulk collection focused on a discrete and insular minority (or if there were no authorizing legislation at all), then a second aspect of the proposed definitions of probable cause and reasonable suspicion—indicating that those determinations "may be based on statistical analysis"—would come into play. Slobogin, *supra* note 96, at 20, 22. As applied to mass collection of records, this language would require a showing that roughly one-half of the records would produce evidence of crime (where probable cause is required) or lead to evidence of crime (where reasonable suspicion is required). *See id.* at 32. Neither showing is likely in the NSA context.