# DOMESTIC SURVEILLANCE OF PUBLIC ACTIVITIES AND TRANSACTIONS WITH THIRD PARTIES: MELDING EUROPEAN AND AMERICAN APPROACHES

by **Christopher SLOBOGIN**, Milton Underwood Professor of Law, Vanderbilt University Law School, Nashville, USA.

In most countries, government surveillance of activities that take place in public is not regulated or only lightly regulated. Similarly, in most countries police efforts to obtain records of everyday transactions usually requires, at most, a finding that the record is "relevant" to an investigation. Arguably, these rules should change now that technology – cameras, drones, computers, and the like – has made both visual surveillance and transaction surveillance easier and cheaper. Technology allows creation of "panvasive" systems that scan across and record the activities of large groups of persons and mining the accumulated data.[1]

On the assumption that a new regulatory regime is necessary, this paper looks to European law as a model for regulating the establishment of panvasive systems, and to American law as a model for regulating government targeting of an individual using such systems. It argues, following Europe's lead, that surveillance systems may not be established unless they are authorized by legislative bodies representative of the affected populace, through specific delegations that require mechanisms for overseeing implementation of the program, all of which is subject to judicial review. It also argues, following suggestions in recent U.S. Supreme Court caselaw, for implementation of "mosaic theory" as a way calibrating the justification required to target the activities or records of a particular individual.

Because it will facilitate the presentation, this paper discusses issues surrounding targeting of particular individuals first, before it examines issues relevant to the creation of panvasive systems. Thus, the first part of the paper discusses mosaic theory and how it might be implemented in a way that meaningfully protects the targets of government investigation. The second part addresses principles that should govern the establishment of the panvasive programs that facilitate such targeting.

[1] The word "panvasive" refers to investigative programs that are both pervasive and invasive, while cutting across large segments of the populace that are largely innocent of wrongdoing. *See* Christopher Slobogin, *Rehnquist and Panvasive Searches*, 82 MISS. L.J. 307, 308 (2013).

## § 1 – Targeted Investigations and Mosaic Theory

In the 2012 decision of *United States v. Jones*[2] the Supreme Court held that month-long tracking using a device planted on a car is a "search" triggering the Fourth Amendment's guarantee against unreasonable searches, and thus (probably[3]) requires a warrant, based on probable cause, before it can occur. The decision was big news in the United States for a number of reasons. First, it introduced the possibility that surveillance of public spaces is governed by the Constitution. Second, it reinvigorated property interests as a basis for Fourth Amendment protection, because it focused on the fact that the tracking in the case was enabled through a trespass on Jones' car.[4] And, of most relevance to this paper, it indicated that at least five justices on the Court are willing to consider some version of what has come to be called "mosaic theory," as a way of figuring out when government information-gathering that normally would not be considered a Fourth Amendment "search" becomes one.

The mosaic idea is captured in Justice Alito's statement, in a concurring opinion joined by three other justices, that "relatively short-term monitoring" of a person's movements on public streets does not implicate the Fourth Amendment but that "prolonged" GPS monitoring does.[5] Justice Sotomayor's separate concurrence went further, stating that the question should be "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits and so on."[6] These kinds of statements are said to be an expression of a mosaic approach to the Fourth Amendment because they suggest that, while collecting isolated bits of publicly available information is not a constitutionally cognizable "search," accumulation and assemblage of numerous discreet pieces can be, because it reveals a fairly good picture about an individual's personal life.[7]

We all can intuit that this is true. Following someone for a few minutes probably won't reveal much, but tracking the person for 28 days, as occurred in *Jones*, probably will. As the lower court in *Jones* stated:

---

2 132 S.Ct. 945 (2012).

3 *Id.*at 954 (explaining that the Court had "no occasion to consider" the government's argument that something less than a warrant based on probable cause would have justified the search in *Jones*).

4 *Id.*at 952 (stating that the dominant test for determining the scope of the Fourth Amendment – which focuses on whether a police action infringes "reasonable expectations of privacy" – "has been added to, not substituted for, the common-law trespassory test").

5 *Id.*at 964 (Alito, J., concurring).

6 *Id.*at 956 (Sotomayor, J., concurring).

7 The first court to apply this term in the Fourth Amendment context was *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010).

Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts.[8]

The same can be said for government perusals of records held by third parties, such as banks, phone companies, internet service providers and credit card agencies. Finding out that an individual has made a particular payment, phone call or email communication can provide some insight into what a person is up to. But a month's-worth of phone and email logs and credit card data is much more likely to reap a gold mine of detail about how one lives one's life.[9]

Nonetheless, until *Jones*, government surveillance of activities in public or of daily transactions outside the home was not governed by the Fourth Amendment, whether short-term *or* long-term. Technically, the same is still true after *Jones*, at least when the surveillance is not aided by a trespass. But a number of lower courts in the U.S. have construed *Jones* to require a warrant for GPS surveillance that is based on cellphone or transponder signals obtainable without a trespass,[10] and some courts, both before and after *Jones*, have required more than a simple subpoena for obtaining certain types of records.[11]

---

[8] *Id. See also*, Jeffrey M. Skopek, *Reasonable Expectations of Anonymity*, VA. L. REV. (forthcoming, 2015) (arguing that the more information the government gathers about individuals, the less anonymous they become, which undermines the right to anonymity).

[9] *See* Steven M. Bellovin, Renee M. Hutchins, Tony Jebara & Sebastian Zimmeck, *When Enough is Enough: Location Tracking, Mosaic Theory and Machine Learning*, 8 N.Y.U. J. L. & LIBERTY 556 (2014) (arguing that the science of machine learning concretely demonstrates how longer-term data collection enhances predictions about behavior and thus allows greater understanding of the person targeted).

[10] *Commonwealth v. Rousseau*, 990 N.E.2d, 543, 553 (Mass. 2103); *State v. Zahn*, 812 N.W.2d 490, 497 (S.Dak. 2012) (holding that putting a GPS device on defendant's car and tracking the defendant was not only a trespass but also infringed his reasonable expectations of privacy); *People v. Weaver*, 909 N.E.2d. 1195, 1201 (N.Y. 2009) (holding, prior to *Jones*, that "[t]he massive invasion of privacy entailed by the prolonged use of the GPS device was inconsistent with even the slightest reasonable expectation of privacy.").

[11] See Stephen E. Henderson, Learning from All Fifty States, How to Apply the Fourth Amendment and its State Analog to Protect Third Party Information from Unreasonable Search, 55 CATH. U. L. REV. 373 424-25 (2006) (describing states that require reasonable suspicion or probable cause to obtain records considered particularly private).

At the same time, however, many courts dealing with the tracking issue have ignored mosaic theory, despite the invitation of the concurring opinions in *Jones* to do so.[12] Rather than gauging whether tracking was "short-term" or "prolonged" they simply require a warrant for all tracking. The major resistance to the theory has not been conceptual, but rather practical. To wit: How is a court to figure out when surveillance is "prolonged"? In the record context, the analogous question might be, how much "aggregation" must occur before the Fourth Amendment is implicated? What if the government only tracks a person for a week rather than a month, or accesses bank records for two different days, separated by a month? As a recent Florida Supreme Court opinion put it, mosaic theory "requires case-by-case, after-the-fact, ad hoc determinations about whether the length of the monitoring crossed the threshold of the Fourth Amendment in each case challenged."[13]

The outcome of this worry about implementation could go in one of two directions. The first is to declare that the Fourth Amendment is usually not applicable in these cases, or at most requires a subpoena based on a minimal relevance showing.[14] The second, endorsed by the post-*Jones* cases noted above, is to state that even minimal surveillance requires a warrant, based on probable cause.[15]

The problem with the first approach – which is in essence the Court's, outside of the anomalous *Jones* decision – is that it blinks at the privacy invasion and governmental abuse that can be associated with suspicionless surveillance. Most of the Court's cases have insisted that we assume the risk that people will see us when we go into public spaces and that a third party to whom we surrender information will hand that information over to the government.[16] But that reasoning is bankrupt, both descriptively and normatively. Most of us don't expect to be subject to prolonged surveillance or monitoring, either visual or

[12] *United States v. Wilford,* 961 F.Supp.2d 740, 771 (D.Md.2013) (noting that "mosaic" theory has presented problems in practice); *United States v. Graham,* 846 F.Supp.2d 384, 401 (D.Md.2012) (same).

[13] *Tracey v. State*, 2014 WL 5285929, *14 (Fl. Sup. Ct. 2014).

[14] Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 315 (2012) (arguing that, "as a normative matter, courts should reject the mosaic theory" and intimating that the author favors a legislative approach).

[15] See cases cited *supra* note 12.

[16] *See, e.g.*, *United States v. Knotts*, 460 U.S. 276, 281-82 (1983) ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another [because he]. voluntarily convey[s] to anyone who want[s] to look the fact that he [is] travelling over particular roads in a particular direction . . . ."); *United States v. Miller*, 425 U.S. 435, 443 (1976) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.");

transactional.[17] Nor should we. As I and others have argued, the Fourth Amendment's promise of "the right to be secure against unreasonable searches" guarantees both a right to anonymity in public[18] and a right to expect that third party institutions to which we surrender information will use it only for its intended purpose; thus, the government should not be able to monitor public movements and transactions with banks, phone companies and the like without justification.[19]

The problem with the second approach – making every act of public or transactional surveillance a search requiring probable cause – is twofold. First, it often will overestimate the privacy invasion; a single location, phone number, or credit charge is usually nowhere near as revealing as the invasions that are classically associated with the Fourth Amendment's probable cause requirement – i.e., ransacking one's home or eavesdropping on phone calls.[20] Second, a rule requiring probable cause for every search handcuffs law enforcement efforts to *develop* probable cause. Much short-term surveillance and many subpoenas for records are designed to get information that will lead to arrest; if the police already had probable cause they wouldn't need the surveillance in the first place.[21]

Thus, mosaic theory – a middle ground between these extremes – makes sense in theory. Moreover, it can be implemented effectively, albeit not perfectly. I have suggested the following time-delineated scheme.[22] For surveillance of public activities that lasts longer than 48 hours, probable cause is required. But for surveillance that lasts less than 20 minutes, police only need to demonstrate a good faith belief that the observation will achieve a

---

[17] *See* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 110-113, 180-186 (2007) (describing studies indicating that many types of public and transaction surveillance are viewed as more intrusive than inspections and frisks that have been held to infringe the Fourth Amendment).

[18] *Id.*at 90-108; Skopek, *supra* note 8, at ___ (arguing that the Fourth Amendment right to be secure from unreasonable searches and seizures encompasses a right to anonymity).

[19] SLOBOGIN, *supra* note 17, at chs. 5 & 7; Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1167 (2002) (arguing for a regime in which, with certain exceptions, "information collected from third party records may only be used for the particular purpose for which it is collected").

[20] *Berger v. New York*, 388 U.S. 41, 63 (1967) (stating that application of the Fourth Amendment's requirements to electronic surveillance "is no formality … but a fundamental rule that has long been recognized as basic to the privacy of every home in America.").

[21] Nina Totenburg, *Do Police Need Warrants for GPS Tracking Devices*, NATIONAL PUBLIC RADIO, Nov. 8, 2011, available at http://www.npr.org/2011/11/08/142032419/do-police-need-warrants-for-gps-tracking-devices (quoting former assistant attorney general asserting that GPS tracking is a useful device for following up leads necessary to develop probable cause); HOWARD W. GOLDSTEIN, GRAND JURY PRACTICE 5-25 (2005) (noting that subpoenas are typically issued "in the context of a preliminary investigation to determine whether any wrongdoing has occurred and whether probable cause exists to charge any individual with commission of any offense").

[22] 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 L. & PUB. POL'Y 1, 24, 28 (2012).

legitimate law enforcement objective. For surveillance that endures longer than 20 minutes but less than 48 hours, reasonable suspicion (a lesser justification than probable cause) is required. Similarly, obtaining records that reflect activity over more than a 48-hour period requires probable cause, but accessing records of activities covering a shorter period of time only requires reasonable suspicion. Under this rule for records searches, probable cause is needed to authorize access to phone or bank records covering more than two days (or more than two days apart), or a record of medical or purchasing history, while obtaining information about a single credit card purchase or headers about a day-long email thread is possible on a reasonable suspicion showing.[23]

This implementation of mosaic theory is based on what I have called a "proportionality theory" of the Fourth Amendment.[24] Proportionality theory already plays a role in the Court's seizure jurisprudence, which allows a detention for up to twenty minutes on reasonable suspicion, but requires probable cause for any detention beyond that, and a judicial determination of cause if the detention lasts more than 48 hours.[25] These distinctions between seizures are based in part on the idea that a stop is less intrusive than an arrest.[26] They are also based on the realization that police need something short of arrest – an investigatory detention – if they are to do their jobs well.[27] The same proportionality approach is justified in the search context. Otherwise, we are left with the extremes: no constitutional regulation at all, or an impossible-to-meet or very watered-down probable cause standard.

Of course, durational limits of this sort are arbitrary means of delineating privacy protection. But the U.S. Supreme Court routinely uses time periods as a prophylactic method of implementing the Constitution.[28] Good examples come from the Court's decisions, just noted, that declare that individuals who are arrested do not need to be brought in front of magistrate unless they are held for longer than 48 hours, and that hold that fifteen to twenty minutes is the threshold for determining when a detention transforms from an investigative stop into a full-blown arrest.[29]

---

[23] Interception of communications would be regulated in the traditional manner, requiring probable cause and a warrant. *See* 18 U.S.C. § 2511.

[24] SLOBOGIN, *supra* note 17, at 21.

[25] *County of Riverside v. McLaughlin*, 500 U.S. 44, 56 (1991) (requiring a judicial determination of probable cause within 48 hours); *United States v. Sharpe*, 470 U.S. 675, 687-88 (1985) (finding a twenty-minute stop reasonable but only because the suspect was responsible for some of the delay).

[26] *Terry v. Ohio*, 392 U.S. 1, 26 (1968) ("An arrest is a wholly different kind of intrusion upon individual freedom from a limited search for weapons").

[27] *Adams v. Williams*, 407 U.S. 143, 145 (1972) ("The Fourth Amendment does not require a policeman who lacks the precise level of information necessary for probable cause to arrest to simply shrug his shoulders and allow a crime to occur or a criminal to escape.")

[28] In addition to the Fourth Amendment rules noted in the text, for instance, the Supreme Court has adopted durational rules in the interrogation context. *See Maryland v. Shatzer*, 559 U.S. 98, 111 (2010) (holding that police may re-initiate questioning two weeks after a suspect requests counsel).

[29] *See* cases cited *supra* note 25.

Statutes also often use duration as a dividing point for privacy protections. For instance, the Electronic Communications Privacy Act requires a warrant for records held on a server less than 180 days but only a showing of relevance after that period,[30] and Title III limits electronic eavesdropping warrants to 30 days.[31] In Europe, France provides several similar examples. For instance, witnesses may be held only for 24 hours without judicial review, and detentions for identity checks are limited to four hours.[32] All of these rules calibrate legal requirements by reference to time periods that, in any given case, could be over or under inclusive. Indeed, in virtually every area of law, prophylactic rules that inexactly effectuate constitutional or legislative intent are common and necessary.[33]

To facilitate implementation of this time-based implementation of proportionality/mosaic theory, I also define probable cause and reasonable suspicion with more precision than traditionally has been the case. Probable cause is defined as an articulable belief that a search will more likely than not produce contraband, fruit of crime, or other significant evidence of wrongdoing, whereas reasonable suspicion is defined as an articulable belief that a search will more likely than not lead to such evidence.[34] Note that both definitions reference a preponderance standard, which is usually associated only with probable cause, not with the less demanding reasonable suspicion concept.[35] In my scheme, reasonable suspicion is still a less demanding justification. But the distinction is achieved not by abandoning the more-likely-than-not standard for an amorphous lower certainty level, but by expanding the type of evidence that may be sought for searches conducted on reasonable suspicion, to include not only obvious evidence of crime, like contraband, but anything that might *lead* to such evidence, such as locational information, a credit card purchase or a phone call.[36]

This differentiation between probable cause and reasonable suspicion – based on the object of the search rather than on the level of certainty that it will be found – provides an additional advantage. As one court has recognized, a significant problem confronted by courts that impose a probable cause requirement on

---

[30] 18 U.S.C. § 2703(a) (2006).

[31] *Id.*§ 2518(5).

[32] *See* Richard Frase, Comparative Criminal Justice as a Guide to American Law Reform: How Do the French Do It, How Can we Find Out, and Why Should We Care? 78 CAL. L. REV. 539, 574-575 (1990).

[33] *See generally* David A. Strauss, *The Ubiquity of Prophylactic Rules*, 55 U. CHI. L. REV. 190, 208 (1988).

[34] Slobogin, *supra* note 22, at 20-23.

[35] *See Terry v. Ohio*, 392 U.S. 1, 22 (1968) ("police officer may in appropriate circumstances and in an appropriate manner approach a person for purposes of investigating possibly criminal behavior even though there is no probable cause to make an arrest.").

[36] *See* generally Christopher Slobogin, Cause to Believe What? The Importance of Defining a Search's Object—Or, How the ABA Would Analyze the NSA Metadata Surveillance Program, 66 OKLA. L. REV. 725 (2014) (arguing that manipulating the object in the way described in the text is the best way to vary justification standards).

GPS tracking is that the locational information obtained is not evidence of *crime*, and thus technically cannot be the target of a warrant as warrants have traditionally been conceptualized.[37] Similarly, as already noted, always requiring probable cause that evidence of crime will be found would prevent the police from carrying out routine investigative techniques, like tracking a person to see if he consorts with a known suspect, contacting a phone company to discover whether he called a suspected co-conspirator on the day of the crime, or acquiring store records to find out whether he purchased a particular type of gun or an item found at the crime scene. The definition of reasonable suspicion outlined above allows such searches to take place (within the 48-hour limit).[38]

My proposal has two other significant components as well. The first is a danger exception that allows relaxation of the usual justification if necessary to *prevent* a serious, specified crime.[39] This exception is based on the idea – well-accepted in Fourth Amendment cases[40] – that when the goal of government intervention is prevention, a somewhat relaxed standard is permissible. But this exception would never apply if the police are trying to solve a crime that has already occurred, nor would it apply unless the crime sought to be prevented is serious and specified.

The second additional component of the proposal addresses an issue that few commentators or courts address: when may surveillance *systems*, designed to facilitate targeting of individuals, be established? For instance, when may the state install a city-wide camera system or a system for monitoring the movements of all vehicles? When may it create data collection systems like the National Security Agency's metadata programs exposed by Edward Snowden, or the "fusion centers" that fill the same role for local law enforcement?[41] That is the subject to which we now turn.

---

[37] *In re Application of the United States*, 2011 WL 3423370, *7 (D. Md. Aug 3, 2011).

[38] This definition of reasonable suspicion also allows what I have called "event-based" investigation, where the police start off with an event, rather than a suspect. SLOBOGIN, *supra* note 17, at 191-192. Say, for instance, police know a murder occurred at a particular location in a park, or that a series of murders with a particular modus operandi occurred in a number of cities, or that a bomb will go off in a particular location at a particular time. Obtaining cellphone or travel log data to determine who was near these locations at the relevant time—the event—could help police zero in on a suspect. While police would not have probable cause as defined above, they would have reasonable suspicion as I define it, at least if the data collection was narrowly constrained by both time and location.

[39] *See* Slobogin, *supra* note 22, at 23 (permitting a search "if a reasonable law enforcement officer would believe [the search] is necessary to help avert [a serious and specific danger]."

[40] *Terry v. Ohio*, 392 U.S. at 26-27 ("a perfectly reasonable apprehension of danger may arise long before the officer is possessed of adequate information to justify taking a person into custody for the purpose of prosecuting him for a crime").

[41] For a description of the NSA metadata program, *see* Glenn Greenwald, *XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet"*, GUARDIAN, July 31, 2013), www.theguadian.com/world/2013/jul/31/nsa-top-secret-program-online-data. For a description of fusion centers, *see* CONSTITUTION PROJECT, RECOMMENDATIONS FOR

## § 2 – PANVASIVE SYSTEMS AND POLITICAL PROCESS THEORY

The two concepts introduced so far – a mosaic theory of privacy protection that requires proportionately greater justification for greater intrusions, and an exception to that rule in cases involving a serious and specific danger – have parallels in European law. European countries recognize that the concept of proportionality is crucial in determining the scope of government's ability to infringe on fundamental rights.[42] And Germany, at least, limits data mining designed to discover more about persons of interest to those situations where the government can demonstrate the mining is in response to serious threat.[43] But, generally speaking, European law is not as well-developed as American law with respect to determining when an individual may be targeted by the government.[44]

In contrast, the European Union has much more attentive, at least in theory, to the predicate issue of when a surveillance system or program may be created in an effort to collect information that can be used to target individuals. In *Digital Rights Ireland*, [45] the European Union Court of Justice held that large-scale retention of data infringes several rights guaranteed in the European Union Charter of Fundamental Rights. It further held that this infringement is justified only if the retention is "strictly necessary" to fight terrorism, organized crime and other serious crime,[46] only if justified by a court or an administrative body that is implementing legislation,[47] and only if the retention is limited durationally and securely.[48]

The *Digital Rights Ireland* case sets out a framework, but is not specific in its directives. German law provides an example of a more specific approach. As Professor Francesca Bignami has noted, in Germany, and to a lesser extent other European countries, a program that indiscriminately vacuums up information about large segments of the domestic population must meet several requirements, even in the national security context. In Germany, for instance, such a program has to be (1) "authorized by a public

---

FUSION CENTERS, available at http://constitution project.org/pdf/fusioncenterreport.pdf (hereafter CONSTITUTION PROJECT).

[42] *See, e.g., Rotaru v. Romania*, App. No. 28341/95, 8 B.H.R.C. 449 para. 43 (May 4, 2000) (construing the Council of Europe Convention and the European Convention on Human Rights, Article 8).

[43] *See Bundesverfassungsgericht* [BVerfG], Apr. 4, 2006, 1 FVerfGE, para. 158 (requiring an "imminent and specific endangerment" of a serious offense, not simply an "abstract endangerment").

[44] For instance, compared to United States law, the warrant and probable cause requirements are diluted and exclusion of evidence is a rarity. *See* Christopher Slobogin, *Comparative Empiricism and Police Investigative Practices*, 37 N.C. J. INT'L L. & COMM'L REG. 321, 323-26 (2011).

[45] Joined Cases C-293/12 & C-295/12, *Digital Rights Irl. Ltd. v. Ministers for Commc'n*, 2014 E.C.R. I-238.

[46] *Id.* at § 56.

[47] *Id.* at § 62.

[48] *Id.* at § 63 & § 66.

law or regulation;" (2) "reviewed, in advance, by an independent privacy agency" and monitored by that agency "to guarantee that the program was being run in accordance with the law"' and (3), as noted above, careful to mine the information acquired "only for certain statutorily prescribed 'serious' threats and, in the case of terrorism, only if there [is] an 'imminent and specific endangerment' from the threat."[49] Further, European law (4) does not permit prolonged detention of the data accumulated and (5) often permits individuals "to check on their personal data, to ensure that it was being used lawfully."[50] Finally, if information is gathered by an intelligence agency, (6) it can only be passed on to domestic law enforcement if a factual threshold of suspicion for a "serious" offense is met.[51]

Compare all of this to the paltry regulation of American mass surveillance programs. Many such programs are either not authorized by legislation or are authorized by legislation in extremely vague terms. For instance, numerous states have established fusion centers, which function like mini-metadata programs, collecting information from federal, state, and local public databases, law enforcement files, and records from private companies in an effort to obtain financial-transaction data, credit reports, car-rental data, utility payments, vehicle identification numbers, and phone numbers.[52] Yet most of these states have not explicitly authorized these centers, and in others the relevant statute merely references the centers without indicating the type of information that may be gathered, the purpose for which it may be obtained, how long it may be retained, means of ensuring its accuracy, or when it may be passed on to officers in the street (items 3-6 above).[53]

Camera surveillance, drone usage and systemic car tracking systems are more likely to be authorized by the relevant legislative body, but again often in vague terms that do not address many of the data

[49] Francesca Bignami, European v. American Liberty: A Comparative Privacy Analysis of AntiTerrorism Datamining, 48 B.C. L. REV. 609, 610-11 (2007).

[50] *Id.*

[51] *Id.*

[52] CONSTITUTION PROJECT, *supra* note 41, at 7.

[53] *See, e.g.*, Tenn. Code Ann. § 67-4-601(7)(B)(i) (in the sole reference to fusion centers, stating that municipal tax funds may be used to establish "high technology systems that collect and share data on criminal activity and historical data with other law enforcement agencies, including fusion centers…"). *See generally*, U.S. SENATE PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, FEDERAL SUPPORT FOR AND INVOLVEMENT IN STATE AND LOCAL FUSION CENTERS (Oct. 3, 2012), available at http://www.hsgac.senate.gov/download/report_federal-support-for-and-involvement-in-state-and-local-fusions-centers (detailing the absence of state regulation of fusion centers and the misuse of fusion center funds by the states, and recommending specific regulations). The federal government has developed privacy guidelines for fusion centers which focus in a very general way on ensuring accuracy of information maintained by the centers, but also make clear that it is up to individual fusion centers to devise their own regulations, consistent with state law. *See* U.S. DEP'T OF JUSTICE, CIVIL RIGHTS AND CIVIL LIBERTIES PROTECTION, August 11, 2008, available at http://www.ise.gov/sites/default/files/CR-CL_Guidance_ 08112008.pdf.

collection and retention issues that should be addressed.[54] At the federal level, while the well-known NSA metadata programs do have congressional authorization,[55] the relevant statute places few limitations on the type of information that may be gathered other than providing that it be useful in protecting national security.[56] Of particular note is the absence – in virtually every state and until recently at the federal level as well – of an independent privacy agency charged with monitoring the implementation of these laws (item 2 above). According to Bignami, European privacy agencies are "policymakers first, enforcers second. . . . Their resources are devoted largely to vetting government proposals for proportionality and making policy recommendations in the face of new technological threats to privacy."[57] These agencies also ensure that the public is told about the effect of any laws that are passed.[58] Although the Privacy and Civil Liberties Oversight Board, reconstituted in 2012, now appears to be fulfilling these roles at the federal level, its oversight authority is limited to national security operations and the extent of its influence remains to be seen.[59]

---

[54] *See* Somini Sengupta, *Privacy Fears Grow as Cities Increase Surveillance*, N.Y. TIMES, Oct. 13, 2013 (cameras), available at http://www.nytimes.com/2013/10/14/technology/privacy-fears-as-surveillance-grows-in-cities.html? pagewanted=all&_r=0 (cameras and drones); Adam Clark Estes, *Why the FAA Isn't Worried Drones Invading Your Privacy Right Now*, GIZMODO, Dec. 12, 2014 (drones), available at http://gizmodo.com/why-the-faa-isnt-worried-about-drones-invading-your-pri-1665794268; Devlin Barrett, *U.S. Spies on Millions of Drivers*, WALL ST. JOURNAL, Jan. 25, 2104, available at http://www.wsj.com/articles/u-s-spies-on-millions-of-cars-1422314779 (car tracking).

[55] 50 U.S.C. § 1861(a), (b) & (c) (authorizing the NSA to collect "any tangible thing" that is "relevant to an authorized investigated … to protect against international terrorism or clandestine intelligence activities," with the authorization to come from the Attorney General or his or her delegate).

[56] One knowledgeable commentator has stated that the statute allows "bulk collection" of all documents and data related to an authorized inquiry, and that the "inquiry" need not focus on a particular crime or suspect, but can instead be a wide-ranging examination of a category of wrongdoing, such as international terrorism. David S. Kris, *On the Bulk Collection of Tangible Things,* LAWFARE RES. PAPER SERIES, Sept. 29, 2013, at 18-20 *available at* http://www. lawfareblog. com/wp-content/uploads/2013/09/Lawfare-Research-Paper-Series-No.-4-2.pdf. ). As I have noted, the guidelines promulgated by the National Counterterrorism Center in 2012 (since modified by presidential directive in substantial ways) allowed the NCTC to "collect, access and retain any piece of information about anyone, and hold it for five years." Christopher Slobogin, *The Future of Mass Dossiers*, JURIST, Apr. 11, 2012, available at http://jurist.org/jurist_search. php? q= Slobogin (commenting on GUIDELINES FOR ACCESS, RETENTION, USE, AND DISSEMINATION BY THE NATIONAL COUNTERTERRORISM CENTER AND AGENCIES OF INFORMATION IN DATASETS CONTAINING NON-TERRORISM INFORMATION, available at https://s3.amazonaws.com/s3.documentcloud.org/documents/ 327629/ nctc-guidelines.pdf).

[57] Bignami, *supra* note 49, at 685.

[58] *Id.* at 648 ("The powers of these national and supranational privacy agencies vary, but most, including the German and French data protection authorities, have the power to review proposed laws and regulations with a data protection impact, to conduct inspections of private and public data processors, and to commence administrative proceedings against violators which may result in injunctive orders or administrative fines.").

[59] According to its website, the Board is responsible for reviewing executive agency actions and legislation, but only in connection with counter-terrorism efforts. *See Privacy*

As I and others have documented, America's failure to institute meaningful oversight of panvasive programs can have concrete repercussions, ranging from erroneous targeting because of data errors to mission creep.[60] Perhaps of most concern, the know-it-all state tends to be a state that oppresses, because officials with knowledge are tempted to use it in any way they can. Congress recognized that fact when it defunded the unfortunately-named Total Information Awareness program in 2003, undoubtedly influenced by the program's eerie icon, depicting an all-seeing eye atop a pyramid accompanied by the logo "Knowledge [Science] is Power."[61] Even the late Chief Justice William Rehnquist, no enemy of strong law enforcement, was leery of such panvasive investigative techniques; as he wrote in 1974 soon after he joined the Court, "most of us would feel that . . . a dossier on every citizen ought not to be compiled even if manpower were available to do it."[62]

As with the targeting issue, there are at least three methods of regulating panvasive surveillance. The most draconian is to ban the creation and maintenance of databases devoted to ensuring the government can develop such dossiers. The opposite extreme is the typical American scheme – either non-existent or loose authorization that leaves virtually all important decisions about the scope and operation of the panvasive system to the executive branch. The third, intermediate, position is to adhere to some version of what I will call the European approach.

Relying on John Hart Ely's political process theory, which posits that only laws that are the product of a properly functioning

---

*and Civil Liberties Oversight Board*, http://www.pclob. gov/about-us.html. In 2014, the Board determined that the NSA's metadata program was *ultra vires* and criticized it on a number of grounds consistent with this paper. *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE U.S. PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 137 et. seq., Jan. 23 2014, available at http://www.pclob.gov/Library/215-Report_on_the_Telephone_Records_Program-2.pdf. To date, however, Congress has resisted ending that program and, according to the Board's latest report, most of its recommendations have yet to be implemented fully. *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, RECOMMENDATION ASSESSMENT REPORT 3-15 (Jan. 29, 2015). Numerous federal agencies have privacy officers, but these officials do not have the power other administrative agencies have to create and enforce rules. Bignami, *supra* note 49, at 686. The principal enforcement mechanism available to these officers is a complaint filed with the Inspector General. *See* 50 U.S.C. § 3029(c).

[60] Christopher Slobogin, *Is the Fourth Amendment Relevant in a Technological Age?* In CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE 11, 19-23 (Jeffrey Rosen & Benjamin Wittes, 2011) (detailing the negative consequences of surveillance briefly noted in the text); Kim A Taipale, *Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd*, 7 YALE J. L. & TECH. 123, 143-59 (2005) (describing abuse, slippery slope and chilling concerns).

[61] *See* Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U.CHI. L. REV. 317, 318-19 (2008) (describing the congressional vote and the influence of the icon).

[62] William H. Rehnquist, Is an Expanded Right of Privacy Consistent with Fair and Effective law Enforcement? Or: Privacy, You've Come a Long Way, Baby, 23 U. KAN. L. REV. 1, 10 (1974).

political process should be considered legitimate,[63] I have contended that the third approach is constitutionally required in the U.S.[64] More specifically, the legality of panvasive surveillance programs should depend foremost on whether they have been authorized by a legislative body that is "representative" of the affected populace (meaning, ideally, that the law applies to those in the legislature and their closest constituents as well as to others).[65] Furthermore, based on what American scholars called the nondelegation doctrine, a program's constitutionality should also depend on the degree to which: (1) the law sets forth an "intelligible principle" that meaningfully guides the executive branch rather than merely delegating all decision-making authority to it; (2) the legislature exercises oversight or requires the executive branch to do so; (3) the executive agency provides reasons for its implementation rules; (4) the rules it establishes are substantively reasonable and well-grounded in fact, and (5) the rules are developed through a notice-and-comment procedure or similarly transparent process (taking into account the need to protect investigational methods).[66] All of this would be enforceable in court.[67]

The simplest way of ensuring that these rules are followed in the U.S. is to ensure that law enforcement agencies follow the dictates of the Administrative Procedure Act (APA) that applies to federal agencies and of similar statutes in the states.[68] Unfortunately, the APA has seldom been applied to law enforcement. As a leading treatise on the subject states, "administrative law includes the entire range of action by government with respect to citizen government interaction, *except* for those matters dealt with by the criminal law."[69] One reason for this position, apparently, is that law enforcement is thought to be just that – law enforcement – and not involved in creating substantive rules like other agencies are. But at least when law enforcement engages in programmatic actions like panvasive surveillance, they are no longer just enforcing the law. Rather they are engaged in policy formation, created by the higher ups in the organization, applying to huge segments of the population, and responding to general problems rather than a

63 *See generally*, John Hart Ely, Democracy and Distrust: A Theory of Judicial Review (1980).

64 Christopher Slobogin, Panvasive Surveillance, Political Process Theory and the Nondelegation Doctrine, 102 GEO. L.J. 1721 (2014)

65 *Id.* at 1733-37 (describing theory and suggesting amendments to it).

66 *Id.* at 1758-65 (describing the nondelegation doctrine and its implications for surveillance programs).

67 *Id.* at 1758-59. Ely subsequently made clear that his theory required legislative authorization in national security matters as well. JOHN HART ELY, WAR AND RESPONSIBILITY: CONSTITUTIONAL LESSONS OF VIETNAM AND ITS AFTERMATH 54-67 (1993) (arguing that the courts should consider whether an authorization for the use of military force is in response to a war or imminent war, and whether Congress has approved the use of force).

68 The federal Administrative Procedure Act is found at 5 U.S.C. § 500 et seq.

69 Kenneth Culp Davis & Richard J. Pierce, J.R., 1 Administrative La Treatise 1 (3d ed. 1994) (emphasis added)

specific incident, as in the usual enforcement scenario.[70] In this setting, the APA should apply.

Although they have never said so explicitly, some judicial decisions have implicitly recognized this point in the investigative context. The Supreme Court has stated that, when warrants are impracticable, courts must ensure that there are "reasonable legislative or administrative standards for conducting an . . . inspection . . . ."[71] As a Utah court stated, "[b]oth warrants and statutes originate outside the executive branch, serving to check abuses of that branch's law enforcement power. In the absence of either of these checks, leaving authority in the hands of police alone is constitutionally untenable."[72]Under this doctrine, unless it has a warrant, panvasive surveillance programs should not be able to operate without the explicit authorization and oversight of Congress and in the absence of implementing rules.[73]

To make all of this more concrete, consider first how a court applying political process theory would analyze an NSA metadata surveillance program aimed at American citizens (the following is a much truncated version of a comprehensive discussion elsewhere[74]). The court would begin by looking at whether Congress has specifically authorized the program; a program created solely at the behest of the executive branch would immediately be viewed as a violation of separation of powers doctrine. Assuming authorizing legislation, the court would examine, in a general way, the scope of the program. If it is aimed at or has the effect of targeting a politically powerless minority, it would be constitutionally suspect.[75] If, instead, it contemplates gathering data on everyone, it would, perhaps counterintuitively, be less vulnerable; if members of Congress pass legislation that will affect them and their constituents in addition to others they presumably will have internalized the costs as well as the benefits of the program. Next, analogous to European law, the court would analyze the extent to which the statute creates independent oversight of the NSA and gives concrete direction to that agency

---

[70] *See generally* Barry Friedman & Maria Ponomarenko, *Governing the Police*, NYU L. REV. (forthcoming).

[71] *Marshal v. Barlow's, Inc.* 436 U.S. 307, 320, 323 (1978); *see also Colonnade Catering Corp. v. United States*, 397 U.S. 72, 77 (1970) ("where Congress has authorized inspection but made no rules governing the procedure that inspectors must follow, the fourth Amendment and its various restrictive rules apply.").

[72] *State v. Sims*, 808 P.2d 141, 149 (Utah Ct. App. 1991)

[73] A central question, raised by David Cole at the conference, is when an action is panvasive and thus triggers process theory's requirements. For instance, if police decide to send a large force into a particular neighborhood, would legislative authorization and implementing regulations be required? The answer depends on how many people are affected and whether the police action is based on evidence or merely designed to collect it. *See* Slobogin, *supra* note 22, at 17-18 (definition of general search).

[74] *See* Slobogin, *supra* note 64, at 1755-58, 1767-74.

[75] One robust indicator of whether a minority is powerless is whether there is a good reason for singling the affected group out for special treatment. *Cf.* Barry Friedman & Cynthia Stein, *Two Types of Policing (Two Protections)* 67-69 (forthcoming, 2015) (advocating for strict scrutiny in such situations).

about the types of data to collect. Finally, it would examine the extent to which the NSA develops implementation rules that are reasonable and developed through a transparent procedure. This last aspect of the analysis would be pre-empted by the Fourth Amendment if, contrary to the Supreme Court's current stance, that Amendment applies in the way outlined in the first part of this article. Even if the Fourth Amendment does not apply, however, the nondelegation aspect of political process theory would allow courts to consider whether, under the totality of the circumstances described by the five factors listed above, the legislative and executive branches have been sufficiently attentive to the demands of democracy.

Political process theory also has implications for American attempts to obtain personal data about people who are not residing in the United States. As construed by the Supreme Court, the Fourth Amendment only applies to aliens who are within the United States and have a significant attachment to it.[76] However, even if this doctrine continues to stand, political process theory provides a basis for arguing that aliens outside the country who are affected by American law can challenge uneven application of that law. As explicated by Ely, process theory entitles citizens from other states to the same guarantees enjoyed by citizens within the state.[77] Although this stance is based on the Fourteenth Amendment's privileges and immunities clause (which speaks of "citizens of the United States") and the equal protection clause (which speaks of persons "within [a state's] jurisdiction),[78] Ely also argued that, as a general matter, courts should be particularly solicitous of discrimination claims by non-Americans, noting that "hostility toward aliens is a time-honored American tradition."[79] Combining these two positions, it can be argued that even foreigners who are not within the United States ought to be accorded privacy protection equivalent to that enjoyed by American citizens.[80] While this protection may not be identical to that provided European citizens by their own countries,[81] it at least

---

[76] *United States v. Verdugo-Urquidez*, 494 U.S. 259, 274-75 (1990) (requiring an individual to have a "voluntary attachment" to the United States in order to be one of the "people" referenced in the Amendment).

[77] Ely, *supra* note 63, at 83-84.

[78] The relevant parts of the Fourteenth Amendment read: "No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; … nor deny to any person within its jurisdiction the equal protection of the laws."

[79] *Id.* at 161. *See also* LAURENCE H. TRIBE, AMERICAN CONSTITUTIONAL LAW 1548-50 (2d ed. 1988) (noting that the Court has required the states to provide strong justification for discriminating against aliens within their jurisdiction).

[80] *Cf. Plyler v. Doe*, 457 U.S. 202, 213 (1982) ("To permit a State to employ the phrase 'within its jurisdiction' in order to identify subclasses of persons whom it would define as beyond its jurisdiction, thereby relieving itself of the obligation to assure that its laws are designed and applied equally to those persons, would undermine the principal purpose for which the Equal Protection Clause was incorporated in the Fourteenth Amendment.").

[81] COUNCIL OF EUROPE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, art. 2(a), Jan. 28, 1981, E.T.S.

prevents Congress from passing laws that allow American law enforcement and national security agencies to infringe foreigners' civil liberties at will, given the protections afforded American citizens.[82] That prohibition would nullify those surveillance statutes that explicitly provide more protection to United States citizens than to foreign citizens outside the country.[83]

## CONCLUSION

The hysteria following 9/11 and the ready availability of mass surveillance technology have been a potent one-two punch that has damaged important civil liberties protecting privacy, autonomy, and self-expression. In working through how to respond to the resulting government enthusiasm for collecting and analyzing any information it can get its hands on, European and American law each have something to offer. Specifically, European law provides a template for regulating the establishment of technologically-sophisticated panvasive surveillance systems, and American law provides a useful model for rules regulating use of those systems to target individuals. This paper has summarized how political process theory strengthens the case for European-style rules governing programmatic surveillance and how proportionality/mosaic theory can improve on the United States' law governing surveillance of individuals.

No. (defining "personal data" that is protected as "*any* information relating to an identified or identifiable individual") (emphasis added).

[82] This position is also consistent with the United Nations' position. *See* U.N. HUMAN RIGHTS COMMITTEE, CONCLUDING OBSERVATIONS ON THE FOURTH REPORT OF THE UNITED STATES OF AMERICA, para 22, http://justsecurity.org/wp-content/uploads/2014/03/UN-ICCPR-Concluding-Observations-USA.pdf (concluding that the right to privacy under the International Covenant of Civil and Political Rights applies extraterritorially).

[83] *See* 50 U.S.C. § 1881a(b)(1-5) (permitting warrantless eavesdropping only if the target is a non-U.S. person who is not located in the United States).