



Reuters/Joshua Lott

Rationalizing Government Collection Authorities: A Proposal for Radical Simplification

By Benjamin Wittes, Wells Bennett, and Rabea Benhalim

The life of every person in an advanced industrialized country is a mosaic of digital information stored on public and private computer servers around the world. Most of the tiles of your own personal mosaic do not reside in your hands. They consist of the electronic fingerprints you leave with increasing frequency over the course of your day-to-day life on computers controlled by third parties: They are the web sites you visit, the toll-booths you pass through, the purchases you make online or with credit cards, the prescriptions you fill, the phone numbers you dial, the emails you send, the library books you take out, the specific pages you have read on your Kindle, the restaurants at which you eat, the photos you post on Facebook, and the photos that others post of you. One can learn more about the average person by taking a comprehensive look at his or her mosaic than by rifling through that person's desk or underwear drawer. Yet our mosaics are composed largely of information that receive dramatically less protection in law and custom than do our homes, cars, and effects.

And here's the rub: Each individual's mosaic—composed, as it is, of the transactions and data that make up his life—is itself only a single tile in the much larger mosaic that makes up modern society and its behavior. That larger meta-mosaic too is being stored, retained, and constantly processed by government, companies, and individuals. The use of the mosaic often works for the individual's own protection—to keep terrorists off of airplanes and to keep credit cards safe from identity thieves—but it can also turn against the individual. The mosaics of non-terrorists keep them off airplanes and out of jobs, for example, and prevent them from getting credit or other benefits.

As a society, we have yet to write coherent or sensible rules governing either a person's own mosaic or the super-mosaic, which constitutes the richest portrait of the collective behavior of a culture ever assembled in the history of the world. In many respects, we have yet to develop even an intellectually compelling way of thinking about the individual and societal interests in amalgamations of non-sensitive trivia which cumulatively paint an intimate portrait. We tend to think about mosaic data in terms of privacy, but this vocabulary does not work well. Much of the material that makes up a person's mosaic involves records of events that take place in public, not in private. Driving through a toll booth and shopping at a store, for example, are not exactly private acts. Only a small fraction of the information in any individual's mosaic is plausibly protected by the Fourth Amendment. Much of it, by contrast, is not protected by any law at all.

In this paper, we look at one corner of the problem of regulating the mosaic—the problem of access by government investigators to individuals' personal data stored in the hands of third parties.

Given the intellectual difficulty of the broad problem of mosaic data, it is perhaps no surprise that our laws in this area are an incoherent mess. The government's authorities to collect the components of a person's mosaic are multifaceted, bewilderingly complicated, and analytically inconsistent with one



Benjamin Wittes is a senior fellow and research director in Public Law at the Brookings Institution. He is also a co-founder of the *Lawfare* blog and has written extensively on the relationship between law and security.

Wells C. Bennett is an Associate at Arnold & Porter LLP.

Rabea Benhalim is an attorney and graduate of the University of Texas at Austin School of Law and the University of Michigan Ford School of Public Policy.

another. Government has a bizarre array of collection authorities that operate under wildly different standards for different types of data. If we are going as a society to develop intellectual and legal strategies for regulating personal data in a pervasively digital society, rationalizing the laws under which government investigators can gain access to individuals' mosaics is a good place to start.

Shortly before he became assistant attorney general in the Department of Justice's National Security Division, David Kris—writing on the modernization of national security surveillance—posed the question of whether the government's national security collection authorities could stand a radical simplification. While acknowledging that the amendments Congress passed to the Foreign Intelligence Surveillance Act (FISA) in 2008 were necessary, Kris worried that the accretion of changes to the FISA over the years had left it relentlessly complicated and thus difficult to apply. Because of its stubborn complexity, he worried, only a tiny coterie of intelligence and legal professionals fully grasp the revised law. Kris wondered whether its ever-increasing density would ultimately serve badly both the needs of government and the civil liberties of those on whom government sometimes wishes to spy.

"FISA has always been an arcane and difficult law," Kris wrote, "but [the new amendments'] intricacy risks confusing the government officials who must apply it, often under substantial time pressure. That can lead to errors of both major types: improperly acquiring communications in a fashion that undermines liberty and privacy and improperly refraining from acquiring communications in a fashion that undermines security." Kris concluded by imagining in broad strokes what he termed "a simpler world in which national security investigations are governed by only two major collection statutes."¹

Kris's observation about FISA actually applies more broadly and highlights a more general problem with the law under which government agencies collect information about individuals. The complexity of the many statutes making up that body of law guarantees a measure of confusion on the part of government, industry, civil liberties groups, and citizens as to the circumstances in which government investigators of various types can and cannot obtain information of various types about people of various types. This complexity in the broader system makes errors likely both in the sense of over-collection and in the sense of under-collection.

More fundamentally, our approach to the shielding of information from government and the availability of information to government reflects no consistent set of policy or philosophical judgments. Considered as a whole, which they very seldom are, these laws reflect few analytically cognizable principles. They are, rather, a haphazard patchwork of authorities and restrictions pieced together over time with different concerns paramount at different times and with very little consideration of the interaction of disparate rules with one another. The

¹David S. Kris, "Modernizing the Foreign Surveillance Act," in *LEGISLATING THE WAR ON TERROR: AN AGENDA FOR REFORM* 234-235 (2009).

degree of protection afforded any given class of information may or may not have anything to do with how sensitive that information is. In some instances, relatively sensitive data receives irrationally little protection; in other instances, relatively trivial data receives dramatically enhanced protection relative to data that might seem much more sensitive to a reasonable person. What's more, the laws often allow the government to obtain the same materials under numerous duplicative authorities using completely different instruments. The standards under which officials may obtain information using these disparate instruments may be similar to one another or may vary a great deal, depending on the authority in question and the type of investigation.

To illustrate this point, consider a scenario that seems as if it would present a simple case: Government investigators in a criminal investigation wish to gain access to records proving that a given investigative subject rented particular videos from a particular vendor. On its face, the law appears to make this pretty difficult. Under the Video Privacy Protection Act, an investigator may only demand production of that record from the video rental agency with a court order, and a court may not order a video business to disclose rental records, unless law enforcement first shows that there is probable cause to believe that the records are relevant to its investigation.² No similar law protects library records, book purchases, or music purchases, all of which prosecutors can obtain merely by asking for them or, faced with an uncooperative vendor, by asserting their relevance to an investigation and giving the vendor a subpoena. Even before proceeding with such a request, the government must notify the affected video customer about its inquiry, even if the notification will prejudice the government's case.³

Yet this remarkably high degree of protection turns out to be something of a mirage. The apparently stringent statute also allows the government to seek the same records with a mere grand jury subpoena under the dramatically lower standard of asserted relevance to a criminal investigation—just like those library records and book and music purchases.⁴ Video records thus receive irrationally high protection relative to other media unless a grand jury happens to be sitting.

What's more, a different procedure entirely applies to stored email communications. Consequently, if investigators merely sought, say, the receipt emailed to the consumer from Netflix, and it sought that receipt from the Internet Service Provider, rather than the rental company, it could circumvent the video privacy law altogether. If the government wants to force a telecommunications company to turn over a subscriber's emails, including such a receipt, then the legal standard will vary depending on what kind of computer the email is stored on, who holds the information, whether the email has been accessed or not, and the

²18 U.S.C. § 2703(b)(2)(C), (3).

³18 U.S.C. § 2710(b)(3).

⁴18 U.S.C. § 2710(b)(2)(c).

email's age.⁵

To summarize the matters as simply as possible, if the government wants to obtain the record from the video rental company, it needs to demonstrate probable cause to a judge (if a grand jury is not sitting) or merely assert the material's relevance (if one is sitting); if it wants to obtain the receipt from the ISP, it needs a search warrant if the email is recent and unopened or a mere subpoena if it is stored in the cloud and is either opened by the user or more than 180 days old.

If none of this makes much intuitive sense, you're not missing some secret unified field theory that binds it all together. It simply doesn't make much sense. The law often suggests a degree of protection utterly disconnected from the protection it affords to comparable data and on which it cannot in practice deliver and therefore does not deliver. It thereby marries obscurity with inconsistency; the principles supposedly guiding this area conflict with one another, and we're not following them anyway.

The system's incoherence is growing more acute as a result of developments wholly unrelated to the legal architecture of surveillance law. Constant technological changes are ensuring that vast new swathes of personal information come within the coverage of existing collection laws. In the years following FISA's passage, for instance, telecommunications companies began to send more telephone signals through undersea cables, and to rely less on satellite transmissions. The shift meant a spike in FISA's application, because the law regulates wire communications more consistently than it does radio communications. Other statutes' regulatory burdens likewise have swelled, as a consequence of the last decade's surge in electronic activity—email, e-commerce, and social networking, to name but a few obvious examples. As more and more personal data gets transmitted, stored, and received, the stakes grow ever higher for the dense and badly-thought-through set of legal rules that govern governmental access to material in the hands of third parties.

This fact is compounded by the ever-increasing government collection effort. Since the September 11 attacks, the government's efforts to collect and process large volumes of information have increased dramatically—and rightly so. There is no comprehensive, unclassified account of these efforts, of how much personal information on American nationals and permanent residents the government has obtained during the last nine years, or even of how much it obtains daily. There is very likely no classified account either. But both because of the increased volume of stored information and because of increased investigative energy, the government clearly now acquires more personal information, from more sources, than it ever has before. And the scope of those collection efforts will only grow further. This trajectory will require more reliance on our flawed matrix of

⁵18 U.S.C. § 2703(a), (b) (requiring government to obtain a warrant before collecting the contents of un-accessed stored electronic communications less than 180 days old, but allowing for the contents of older communications, and the contents of accessed communications stored in remote computing services, to be collected with a subpoena.)

collection authorities, and a heightened risk of the problems Kris identified: inappropriate collection and use of protected data and inappropriate failures to collect information essential to securing legitimate government interests.

All of which raises the broad question which Kris posed narrowly about FISA: Is it possible to imagine a simpler world in which government collection authorities reflect a coherent, mutually consistent set of principles?

Our purpose in this paper is both to describe the incoherence of the system that has developed over time and to sketch a strategy for its radical simplification. We focus here on only one corner of the problem: Data about, owned by, or controlled by individuals yet stored in the hands of third parties. We do not treat in any detail either real-time surveillance under any of various statutes or searches covered by the Fourth Amendment. We are concerned here, rather, with government access to the mosaic, not chiefly with real-time communications—that is, with government access not to transient conversation but to the permanent fingerprints of proliferating types that people leave throughout each and every day. Our goal is not to review existing collection laws exhaustively, much less to offer a detailed roadmap to comprehensive reform. It is, rather, to describe the modern system of government collection authorities as a system, to ask whether it makes sense—or, more precisely, to identify the specific areas where it does and the other areas where it does not. Such an understanding of the system as an organism, we believe, gives rise to policy options towards a simpler, more integrated and philosophically sensible collection regime, one that ensures public goods to the greatest extent possible while identifying precisely the privacy and civil liberties interests it means to protect and then rigorously protecting them.

Specifically, we mean to argue that American collection should be reorganized to accomplish three objectives: First, to protect more rigorously data making up the personal communications and materials of individuals stored in the cloud; second, to stop pretending to rigorous yet ultimately fictitious protections of routine transactional data of various sorts and to reorganize such protection to at once encompass a broader array of data and to design a streamlined and uniform administrative subpoena apparatus to give investigators access to such data; and third, to designate certain discrete types of transactional data as especially sensitive and warranting heightened protection.

The Logic of the System

The American collection architecture has a crude logic to it. It is, broadly speaking, a modified logic of the Fourth Amendment. As former Department of Homeland Security policy chief Stewart Baker has argued:

The way lawyers and judges think about privacy has been conclusively shaped by the Fourth Amendment to the U.S. Constitution. That amendment guarantees the privacy of citizens by confirming their right to be “secure in

their persons, houses, papers, and effects against unreasonable searches.” This right is protected by requiring that searches be approved in advance by independent judges who issue search warrants on the basis of sworn statements stating the “probable cause” for the search.

As new technologies emerged—and offered new sources of information about citizens—privacy advocates sought to squeeze law enforcement access to the new information into this standard “search” model.

...

Most of these enactments are derived from the “search” model and offer some kind of watered-down Fourth Amendment protection. That is, the government is allowed access to information in a third party’s hands if the government can obtain some kind of legal process (*e.g.*, a subpoena or court order) based on some kind of predicate set of facts (*e.g.*, the data is “relevant to an ongoing investigation.”)⁶

The result is that collection statutes generally share to a certain degree a common set of structural and normative assumptions. The system, made up of the aggregation of these laws, is consequently not entirely devoid of overall rationality or sense of purposeful design. Generally speaking, collection statutes tend to encompass variants of the following four principles.

First, they presume that the government does not have access to individuals’ personal information. This may seem like an obvious point, but it’s not an inevitable structural feature of collection law. One could imagine, for example, an alternative legal world in which the government had a great deal more latitude to collect as an initial matter—say, the authority to order companies to produce personal data on request—and where privacy protections lay principally in the restrictions on the use, misuse, and dissemination of that information. Such restrictions already constitute a significant feature of our larger surveillance rules, of course, but one could imagine them playing a far greater role *relative to restrictions on collection itself*. One could also envision a regime, like that in some other democratic countries, that simply gives the government a freer hand.⁷ But these are not the models that our collection statutes have followed. Rather, their model, as Baker suggests, is the Fourth Amendment. And that is a model that *presumes non-access*. For the most part, American collection law thus takes as its starting point

⁶Stewart A. Baker, “The Regulation of Disclosure of Information Held by Private Parties,” in *PROTECTING AMERICA’S FREEDOM IN THE INFORMATION AGE* 161 (2002).

⁷See Mark Gitenstein, “Nine Democracies and the Problems of Detention, Surveillance, and Interrogation,” in *LEGISLATING THE WAR ON TERROR: AN AGENDA FOR REFORM* 31-32 (2009) (noting that Israeli police may monitor telephone calls originating in Gaza or the West Bank without seeking a prior court order; and that while court orders are required for wiretaps on Israeli soil, courts often automatically grant police requests for wiretap orders); see also generally Gary J. Schmitt, *SAFETY, LIBERTY AND ISLAMIST TERRORISM: AMERICAN AND EUROPEAN APPROACHES TO DOMESTIC COUNTERTERRORISM* (2010).

the proposition that personal information lies beyond the state's reach.

Second, as with the searches and seizures the amendment directly regulates, collection statutes generally permit the government to overcome the presumption against its collection of individuals' personal information only if it is prepared to defend a predicate factual showing before a judge. That is, they require a showing of some sort to a court either before an order can issue directing the material's production or in retrospect in defense of such an order. The standards will vary for this showing—as will the procedures for it—according to both the nature of the government's inquiry and the nature of the information in question. But as a general matter, the government cannot demand information simply because it wants it. It can demand it only because something justifies its acquisition. For authorities and citizens alike, therefore, the most pressing and recurrent question is what legal test the government will have to meet before it can start collecting.

This model is woven into the collection system at many different levels—for wiretaps as well as for collection of records from third parties. Unless authorities first demonstrate probable cause to the FISA Court that a Canadian tourist in Utah is an agent of Al Qaeda, for example, they cannot commence intelligence surveillance of that tourist's cell phone conversations.⁸ Wiretaps are likewise permissible in the criminal context only after law enforcement officers have made a predicate factual showing akin to probable cause.⁹ Authorities can get pen register and trap-and-trace orders, but only after applying to a judge and showing that the information likely to be obtained is relevant to a criminal investigation.¹⁰ The FBI can issue national security letters without prior court approval to receive financial, credit history, and electronic communications data based on the material's claimed relevance to a national security investigation, but the recipient can move to quash it in court, and the government will then have to defend its propriety.¹¹ Similarly, a prosecutor can issue a subpoena on behalf of a grand jury if he believes that there is a reasonable possibility that the subpoena will lead to the discovery of relevant information—a claim the recipient can then challenge in court.¹²

These examples illustrate the diversity of collection standards, but they also illustrate some common threads and hint at a degree of legislative logic over time concerning how to organize collection rules: Not only does the government lack presumptive access to personal data in the hands of third parties, but it garners such access by clearing evidentiary hurdles.

Third, even where the government acts lawfully in collecting personal

⁸50 U.S.C. §§ 1801(f), 1805(a)(2)(A)-(B).

⁹18 U.S.C. § 2518(3)(a).

¹⁰18 U.S.C. §§ 3122 (b)(2), 3123(a)(1).

¹¹12 U.S.C. § 3414; 15 U.S.C. § 1681u-v; 18 U.S.C. § 2709.

¹²FED. R. CRIM. PROC. 17; *see also United States v. R. Enterprises, Inc.*, 498 U.S. 292, 301 (1991) (court will only quash grand jury subpoena on relevance grounds if the recipient can show that there is no reasonable possibility that the subpoena will produce information relevant to the general subject of the grand jury's inquiry).

information, other rules may nonetheless limit disclosure to government by third parties of personal information. Collection laws comprise not just rules for when and how the government may obtain data about individuals. These also often regulate the behavior of the third party holding the material. The result is that rules running parallel to the government's authority to request information may limit a third-party's legal ability to comply with that request. For example, Comcast is prohibited from divulging information about the cable viewing habits of its subscribers to police (or to anyone else) unless the company has received a special court order.¹³ Similar rules regulate the extent to which schools, hospitals and video rental business may turn over third party information to investigators.¹⁴ These entities share the feature barring the unilateral dissemination of personal information, except according to specific procedures defined within the laws themselves.

Conversely, a vast array of personal information is not subject to protective regulation at all; to take an easy example, a bank may voluntarily turn over an ATM camera recording of a customer, who makes a withdrawal but then is filmed while threatening another customer with a firearm. The bank may do so whether or not the police have asked the bank for any records, and the police may ask for such information without any evidentiary predicate. There are also a few narrow categories of information that third parties *must* provide to the government—automatically and without any request—in order to ensure public safety. Despite confidentiality rules, many professionals are obligated to inform the authorities if their clients express a credible intention to harm themselves or others; health organizations likewise must hand over certain patient information to federal regulators, when the latter investigates potential violations of federal health privacy law.¹⁵

And there are cases as well in which government collects information in bulk with no predicate factual showing, generally for national security purposes. Under the FISA Amendments Act, for example, the government may scoop up communications and meta-data indiscriminately as long as the targets are “reasonably believed” to be non-U.S. persons overseas.¹⁶ Federal law and

¹³47 U.S.C. § 551 (c)(2)(D), (h).

¹⁴*See, e.g.*, 20 U.S.C. §§ 1232g(b)(1) (withholding federal funds from educational institutions which, as a matter of policy or practice, disclose certain classes of educational records and related information), 1232g(b)(1)(J)(i)-(ii) (allowing for educational institutions to disclose students' educational records, upon issuance of a grand jury subpoena or similar request); 18 U.S.C. §§ 2710(b)(1), (c) (imposing civil liability on video service providers that disclose customers' personally identifiable information and providing for cause of action), 2710(b)(2)(C) (allowing for disclosure to law enforcement upon presentation of lawful requests); 45 C.F.R. §§ 164.510 (precluding disclosure of third party health records unless affected person has an opportunity to object), 164.512 (allowing for certain disclosures of third party health records without affording the affected person an opportunity to object, including upon presentation of requests from law enforcement officials).

¹⁵45 C.F.R. § 164.502(a)(ii).

¹⁶50 U.S.C. § 1881a(a).

regulations authorize the bulk collection of passenger reservation records for international flights with one end in the United States.¹⁷ And the Treasury Department has, since September 11, collected in bulk certain banking transaction records from a Belgian consortium called SWIFT.¹⁸ In such cases, the normal logic of the system is suspended out of some combination of the imperative demands of security, the non-investigative nature of the inquiry, and the inapplicability of the Fourth Amendment model to foreigners overseas.

Such cases, in any event, represent the exceptions to the more general rule, which is that companies have duties to protect certain classes of information. And by and large, the statutes that circumscribe third party disclosures proceed on the same assumption as do the statutes that authorize government collection: that personal information is presumptively not accessible by the state (or the public) and that the third party must therefore not release it *unless the state meets a certain evidentiary predicate*.

Fourth, the government may suffer penalties when it collects personal information outside of its explicit legal authorities. When the State's activities are covered by the Fourth Amendment, failure to comply with proper procedures can result in the exclusion of the collected information from evidence in court proceedings or in a lawsuit against the collecting official. Similar mechanisms show up in many collection statutes. In the most direct parallel, Congress wrote an exclusion remedy into the Video Privacy Protection Act, which bans all courtroom use of video rental information not obtained in accordance with the Act;¹⁹ the federal wiretap statute has a similar provision, and furthermore authorizes courts and executive agencies to discipline any officers who intercept telephone calls illegally.²⁰ And though they do not employ exclusionary rules, both the Stored Communications Act and the Foreign Intelligence Surveillance Act provide for civil actions against the United States, if only in cases in which the government willfully violates specific rules contained in those statutes.²¹ More stringently, the Right to Financial Privacy Act creates a cause of action against the United States when the illegal collection or disclosure of financial information is the product of mere negligence; willful violations also can mean workplace discipline for individual government agents.²²

The recurrence of these basic features across collection regimes— together with

¹⁷49 U.S.C. § 44909(c)(3); 19 C.F.R. § 122.49d(a).

¹⁸See Executive Order 13,224, 66 Fed. Reg. 49079 (Sept. 25, 2001); 31 C.F.R. §§ 594, 501.602; see also "Legal Authorities Underlying the Terrorist Financing Tracking Program," available at <https://ustreas.gov/press/releases/reports/legalauthoritiesofftp.pdf> (last visited on Dec. 20, 2010) (explaining Department Treasury's invocation of Executive Order and federal statutes and regulations, as bases for collection of SWIFT data).

¹⁹18 U.S.C. § 2710(d).

²⁰18 U.S.C. §§ 2515, 2518(10)(a), 2520(f).

²¹18 U.S.C. § 2712(a) (providing civil remedy for willful violations of both SCA and certain provisions of FISA).

²²12 U.S.C. § 3417(a), (b).

the other recurrent features described above—point to some non-trivial degree of logic to the system. Clearly, Congress has repeatedly sought both to deter the worst forms of unlawful collection, to ensure that government has a reason to acquire third-party-held data, and to provide remedies to individuals whose personal information is obtained or disseminated improperly.

The Irrationality of the System

To acknowledge that a crude logic underlies our complex system of collection law, however, is not to say that this body of law has the sort of internal coherence for which one would hope. Yes, the system has a few recurrent features, most importantly an assumption that the government usually must be prepared to make a predicate factual showing before it can access personal information. And yes, those features tend to have roots in the same source: an importation of the logic and structure of the Fourth Amendment to those areas which it does not cover but which seem similar enough to the matters that it does cover such that some facsimile—robust or faded—of Fourth Amendment protection is required. But the logic and philosophical consistency of the system in its application of these larger principles, or indeed of any principles, is skin deep. On any closer inspection of the statutes in question, a number of anomalies and oddities emerge, and the system quickly comes to resemble a patchwork, not a system at all.

To illustrate this point, let's return to the hypothetical case of an emailed copy of a purchase receipt, this time one sent to your personal email account moments ago by a clothing store's website. Assuming you have not yet opened this email, its contents are protected by the Stored Communications Act, which applies a relatively robust regime: Neither your internet service provider nor the store's may hand over the email's contents—its text or any images within it—unless the government first presents one or both of them with a warrant issued by a judge on a showing of probable cause.²³ Yet the same transaction also generates a record of your purchase. Under the Right to Financial Privacy Act, that record can be collected from your bank in four different ways, if the government thinks that the record might be relevant to a criminal case—though this order would yield only a record of the financial transaction, not the item purchased.²⁴ A grand jury may also send you or the store a subpoena, thus invoking perhaps the least demanding standard from the government's point of view.²⁵ And if you happen to open the

²³18 U.S.C. § 2703(a); *see also generally* Orin Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," 72 GEO. WASH. L. REV. 1208 (2004).

²⁴12 U.S.C. §§ 3405-3407, 3413(i) (providing for mandatory disclosure of financial records, upon presentation of a search warrant, an administrative subpoena, a judicial subpoena, or a grand jury subpoena).

²⁵*United States v. R. Enterprises, Inc.*, 498 U.S. 292, 301 (1991) (court will only quash grand jury subpoena on relevance grounds if the recipient can show that there is no reasonable possibility that the subpoena will produce information relevant to the general subject of the grand jury's inquiry).

email and nonetheless maintain it on a remote server, the standard under the Stored Communications Act too plummets, and a subpoena will suddenly suffice. In a national security investigation, the FBI can also issue a national security letter to the bank or to the Internet company for details surrounding the email's transmission or the purchase recorded online.²⁶ There are, in short, myriad different ways for officials to learn that you recently spent \$34.95 on a nice new outfit from Macy's—each varying in form and substance, sometimes greatly so. Some of these distinctions make sense. Many do not.

The system has several distinct axes of irrationality—a few of which are visible in this example. First, there are the cross-cutting collection authorities pursuant to low standards that function as rule-eating exceptions to more robust privacy regulations. Second, where these cross-cutting legal authorities are not available, the standards and procedures for the acquisition of the same information are not consistent. And third, some laws give heightened protections to less sensitive material, while more sensitive material remains acquirable under depressed standards. Let us consider each of these three points in turn.

The first point is that many of the system's apparently robust anti-disclosure protections get consumed by exceptions—lenient, government-friendly collection methods. While statutory law specific to individual data-types often obligates the government to meet some demanding standard before it can access personal data, these will tend to have loopholes, and the system's architecture is such that one of these exceptions will almost always apply, at least in criminal or national security investigations. That, in turn, permits the government to acquire information upon meeting a much-more-forgiving standard in all of the most common scenarios.

The source of this anomaly is not subtle. Three cross-cutting collection mechanisms collectively enable the government to obtain a great deal of personal data according to particularly undemanding standards. The national security letter and the order for business records under the FISA, the first two of these authorities, have both sparked great controversy and attention. But it is actually the third, the grand jury subpoena—which is relatively uncontroversial—that provides the most powerful acquisition authority.

The term “national security letter” (NSL) is shorthand for a type of administrative subpoena, issued by the executive branch without prior judicial approval in national security investigations. The recipient typically cannot discuss with or acknowledge to anyone except an attorney having received an NSL, which can cover a limited range of not-especially-sensitive material. With an NSL issued under the Electronic Communications Privacy Act (“ECPA”), the government can require communications companies to disclose telephone subscriber information, defined as the subscriber's name, address, the length of his or her service, and any records required to bill the customer for local and long-distance telephone calls. The same companies may, in the government's view of the law, be ordered to

²⁶18 U.S.C. § 2709.

produce transactional records for emails, similarly understood to mean the subscriber's name, address, service duration, and records necessary for billing.²⁷ Also, under the Right to Financial Privacy Act ("RFPA"), the government may use NSLs to command financial institutions to turn over individual financial records, broadly defined.²⁸ The Fair Credit Reporting Act ("FCRA") lastly authorizes the government to order credit bureaus to disclose their customers' identifying information, or information identifying the customers' banks and financial institutions.²⁹

NSLs vary slightly in their mechanics. An NSL for electronic communications information only may issue if the executive branch certifies to the recipient that the materials sought are relevant to a counterintelligence or counterterrorism investigation.³⁰ By contrast, an NSL may compel the disclosure of financial information if such information is desired for the "purpose" of protective operations carried out by the Secret Service, or for counterterrorism, counterintelligence, or foreign intelligence-gathering, by an agency authorized to perform those activities.³¹ Credit reporting information is also subject to a slightly different (and perhaps lower) standard: customer identifying information, and the identity of customers' financial institutions must be disclosed to the Federal Bureau of Investigation pursuant to an NSL, if the appropriate official certifies that such data is sought for the "conduct" of an authorized counterterrorism or counterintelligence investigation.³² Other authorized agencies may obtain the same information for counterterrorism purposes, if they certify that it is "necessary for the agency's conduct or such investigation, activity or analysis."³³

The practical difference between these lesser, purpose-driven standards and "relevance" can be debated. But even assuming that the latter is marginally more restrictive than the former, the NSL standard still can be fairly characterized as relevance, as determined by the very agency seeking the production: presumably, the government would not intentionally collect obviously irrelevant national

²⁷ 18 U.S.C. § 2709(a)-(b); *see also* Memorandum from Daniel Koffsky, Deputy Assistant Attorney General, to Valerie Caproni, General Counsel, Federal Bureau of Investigation, re: "Requests for Information Under the Electronic Communications Privacy Act" 3 n. 3 (Nov. 5, 2008) (noting, in view of legislative history, that ECPA's NSL provision reaches electronic communications data "parallel to subscriber information and toll billing records for ordinary telephone service."). There is an ongoing controversy concerning whether and how the NSL authority reaches email, however. *See* Ellen Nakashima, "White House Proposal Would Ease FBI Access to Records of Internet Activity," WASH. POST (Jul. 29, 2010).

²⁸ 12 U.S.C. §§ 3414 (authorizing government to compel disclosure of financial records by issuing a national security letter); 3401 (defining "financial record" as "an original of, a copy of, or information known to have been derived from, any record held by a financial institution pertaining to a customer's relationship with the financial institution.") (emphasis added).

²⁹ 15 U.S.C. § 1681u-v.

³⁰ 18 U.S.C. § 2709(b)(1).

³¹ 18 U.S.C. § 3414(a)(1)-(3).

³² 15 U.S.C. § 1681u(a).

³³ 15 U.S.C. § 1681v(a).

security information.³⁴ In any event, the NSL's undemanding standard of "relevance or less," together with the absence of any prior judicial review, allows the government to collect materials covered by NSLs with great ease. While NSLs are among the more controversial of the government's collection authorities, their use is generally limited to relatively non-sensitive data, material that in other contexts does not receive heightened protection anyway. So their use does not generally have the effect of lessening the standard the government needs to reach in order to acquire data. It does, however, have the effect of altering the bureaucratic framework required for production. NSLs allow the investigative agencies to demand material on their own authority. Grand jury subpoenas, by contrast, must go through the Justice Department, making investigators answerable to prosecutors.

It is nearly as easy substantively, though most definitely not bureaucratically, for the FBI to obtain a far broader range of business records for intelligence or counterterrorism purposes under the Foreign Intelligence Surveillance Act ("FISA"). Under FISA, a judge of the Foreign Intelligence Surveillance Court ("FISC") may approve an *ex parte* order compelling the production of "any tangible thing," provided the government convinces the judge that the desired items are relevant to an authorized investigation "to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."³⁵ FISA helpfully deems the requested tangible things to be "presumptively relevant" if they pertain to a foreign power, their agents, or persons in contact with foreign powers or their agents. That lessens the government's burden, practically speaking, given that FISA proceedings are *ex parte* and held in secret, and thus do not afford the affected party (or anyone other than the judge) an opportunity to rebut the presumption of relevance.³⁶

³⁴At least one arm of the Government – at one time – suggested that *all* NSLs should be subjected to some sort of internal relevance review. Just after 9/11, the Federal Bureau of Investigation required its investigators, before issuing an NSL, to describe the relevance of any sought materials to supervisory personnel, regardless of whether of the legal standard imposed by the applicable authorizing statute. See Memorandum from the Office of the General Counsel to All FBI Field Offices re: "National Security Letter Matters" at 6, 7 (Nov. 28, 2001) (explaining, among other things, that required internal memorandum assists NSL process by setting forth "why the information sought is relevant to an investigation;" and that, because of changes introduced by the passage of the USA PATRIOT ACT, NSLs may issue upon a "certification of relevance.")

³⁵ 50 U.S.C. § 1861(b)(2)(A), (c)(1). In the case of the "an application for an order requiring the production of library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person," the law requires that the FBI director not delegate his authority to request this material below the level of either the deputy director or the executive assistant director for the bureau. See 50 U.S.C. § 1861(a)(3).

³⁶ 50 U.S.C. § 1861(b)(2)(A)(i)-(iii) (tangible things presumed relevant if the government's statement of facts demonstrates that the tangible things "pertain" to a foreign power; an agent of a foreign power; the activities of a suspected agent of a foreign power who is the subject of an authorized

While the government may issue NSLs unilaterally, it must persuade a FISC judge before obtaining an order for business records; and in that respect, the FISA collection authority is far more stringently regulated. But the substantive standard is basically the same relevance standard that applies to NSLs. And like the recipient of an NSL, a business record order's recipient can be "gagged" and prohibited from acknowledging the order's existence, or talking about it to third parties other than lawyers. Recipients also have limited rights to challenge orders for production and non-disclosure, and such challenges are most unlikely to succeed. A judge of the FISC can only quash an order for business records if it does not satisfy the quite-lenient rules set forth above; and non-disclosure orders likewise only will be set aside if the judge improbably finds there is no reason to believe that doing so would harm the national security.³⁷ The judge must furthermore treat as conclusive the executive branch's good-faith suggestion that such harm, or harm to diplomatic affairs, would result from disclosure.³⁸

The most powerful cross-cutting collection authority of all is the grand jury subpoena—involving at once the least stringent standard, only modest bureaucratic obstacles, and a particularly broad range of accessible data. The principle that the grand jury is entitled to every man's evidence is old and venerable. But in a world in which we leave mosaic records of so much of our lives in the hands of third parties, we should be frank about its consequences. The grand jury subpoena has become a surveillance tool of enormous power. Using this tool, prosecutors may acquire nearly any data in the hands of third parties—save certain discrete categories of data concerning ongoing communications—in spite of rules that preclude dissemination of, for example, financial, credit, health, video, and educational information. The standard is subtly lower than relevance, for the Supreme Court has said that when "a subpoena is challenged on relevancy grounds, the motion to quash must be denied unless the district court determines that 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."³⁹

The statutes regulating government access to specific types of data all permit grand juries to subpoena third parties' personal information, and they do not

investigation; or an individual in contact with or known to a suspected agent of a foreign power who is the subject of an authorized investigation). Of course, the government's power to obtain business records is broader with respect to foreigners than it is with respect to "U.S. persons" – citizens and other lawfully authorized residents of the United States. As far as U.S. persons are concerned, the government may apply to the FISA court for an order for business records, only if the relevant intelligence investigation is "not conducted solely upon the basis of activities protected by the first amendment to the Constitution." 50 U.S.C. § 1861(a)(1).

³⁷50 U.S.C. § 1861(f)(2)(C)(i)-(iii).

³⁸50 U.S.C. § 1861(f)(2)(C)(ii).

³⁹*United States v. R. Enterprises, Inc.*, 498 U.S. 292, 301 (1991) (emphasis added).

significantly restrict the recipients' ability to comply.⁴⁰ Only the electronic communications and cable laws materially cabin the subpoena's reach, and then only to modest degrees. As we explained above, if a stored electronic communication, such as an email, is less than six months old and unopened, then the grand jury cannot compel an electronic communications provider to produce the email's contents. But after that point or if opened, email contents are subject to subpoena, with modified notice procedures.⁴¹ The cable statute imposes a gentler regime on cable companies, which are prohibited only from disclosing their customers' specific programming selections in response to a grand jury subpoena. For that, prosecutors need a special court order.⁴² (Electronic communications providers and cable businesses—which are often one and the same, since firms like Comcast and RCN often provide both cable television and internet services—can always produce such basic subscriber information as customer identifying data, address in response to grand jury subpoenas.⁴³)

The grand jury subpoena is not broadly controversial among civil libertarians. This is strange. It is a far more powerful instrument, more generous to the government and in some respects less solicitous of privacy, than other collection mechanisms. It does not have the same strict limitations on the types of records accessible as do national security letters, nor does it require advance judicial review, as do FISA orders for business records. Procedurally, the decision to issue the subpoena is the prosecution's alone. While the grand jury subpoena, as noted above, requires as a bureaucratic matter the involvement of a prosecutor before the government can make a production demand, that frequently means in practice a lone Assistant United States Attorney. Indeed, a federal prosecutor often can issue a grand jury subpoena without having to seek permission from supervising attorneys, or to convince anyone that the subpoena complies with legal requirements.⁴⁴ That distinguishes the grand jury subpoena from certain forms of national security letter, which cannot issue until investigators certify that the sought items are indeed relevant to or necessary for a specifically-defined national

⁴⁰15 U.S.C. § 1681b(a)(1); 35 U.S.C. § 3414(i); 45 C.F.R. § 164.512(f)(1)(ii)(B); 18 U.S.C. § 2710(b)(2)(C); 1232g(b)(1)(J). Regulations promulgated under the Health Information Portability and Accountability Act ("HIPPA") authorize health providers to disclose protected health information pursuant to a grand jury subpoena. 45 C.F.R. § 164.512(f)(1)(ii)(B). However, HIPPA also permits the states to enact more stringent privacy protections, in certain contexts – and in Ohio, communications between doctors and patients are absolutely privileged from disclosure. A federal court relied on that rule, in concluding that the former target of a grand jury investigation could sue a hospital for disclosing health information sought by federal investigators. *Turk v. Oiler*, No. 09-CV-381 (N.D. Ohio, Feb. 1, 2010).

⁴¹ 18 U.S.C. § 2703(b).

⁴² 47 U.S.C. § 551(c)(2)(D).

⁴³ 18 U.S.C. § 2703(c)(2).

⁴⁴According to Justice Department policies, prosecutors must obtain permission from senior officials, if they wish to issue a grand jury subpoena for certain narrow categories of personal data, such as information bearing on the fees charged by attorneys, or information in the hands of the news media. See U.S. Attorney's Manual § 9-11.255.

security investigation.

On the other hand, grand jury subpoenas are more open than FISA business record orders and NSLs, and a recipient can challenge them openly in court. But that can happen only after the issuance of the subpoena, the commencement of litigation, and almost invariably, the retention of a costly attorney. What's more, courts generally will only quash or modify a challenged grand jury subpoena if it is too vague, exceedingly burdensome, or 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."⁴⁵ The burden of proving that negative falls on the subpoena's recipient; the government does not bear the burden of proving its subpoena is reasonable or well-tailored.⁴⁶

All of this means that the government can generally obtain personal data in any criminal investigation with very little hindrance from the many statutes that seem to impose barriers. For example, the Right to Financial Privacy Act ("RFPA") generally shields your financial information—records of your check card transactions, account numbers, and the like—from disclosure by Wachovia or Bank of America or any other financial institution where you hold an account.⁴⁷ And under normal circumstances, the RFPA allows for compulsory access to these records if the government makes a showing of probable cause to a judge.⁴⁸ But that protection turns out to be a mirage, because the RFPA also allows for compulsory, as well as voluntary disclosure to the government, provided that the government has reason to believe that the records in question will be relevant to a criminal investigation.⁴⁹ And it furthermore permits access with a grand jury subpoena. Add to this the other rule-eating exceptions described above—national security letters and a business records order issued by the FISC—and the promise of financial privacy starts to look like a bit of an illusion. The real rule is that your bank data are private, absent your consent, unless the government seeks discovery according to one of RFPA's four discovery procedures. Or unless your bank records are sought for counterintelligence or counterterrorism purposes—and are therefore subject to mandatory, gagged disclosure upon receipt of an NSL. Or unless the records are relevant, or deemed presumptively relevant to a counterintelligence or counterterrorism inquiry and are therefore subject to mandatory, gagged disclosure pursuant to a FISA business records order. Or unless a prosecutor decides, without informing her superiors or anyone else that your banking records are relevant to her investigation. Thus, despite its lofty suggestion to the contrary, the law ensures that in almost any real-world investigative situation, your check card data will be handed over to authorities with minimal or no prior judicial review, and on a showing of mere relevance.

⁴⁵*United States v. R. Enterprises, Inc.*, 498 U.S. 292, 301 (1991).

⁴⁶*United States v. R. Enterprises, Inc.*, 498 U.S. 292, 301 (1991); FED. R. CRIM PR. 17(C).

⁴⁷12 U.S.C. § 3402.

⁴⁸12 U.S.C. § 3406(a).

⁴⁹12 U.S.C. §§ 3402(1)-(5); 3404-3408.

That is not in our judgment bad policy, but its obscurity is certainly bad policy.

The prevalence and sweep of these cross-cutting collection techniques—NSLs, FISA business records orders, and particularly grand jury subpoenas—creates a bizarre anomaly in the collection architecture: These mechanisms are not available to federal authorities all of the time. The issuance of an indictment, for example, forecloses resort to a grand jury subpoena as an evidence gathering tool; NSLs, as noted above, may only be used with respect to certain discrete classes of information related to electronic communications and financial and credit reporting information. When investigators cannot invoke these less burdensome authorities, they must acquire information by other, more demanding means. Absent a grand jury subpoena, for example, prosecutors may have to seek a court order for the production of cable television information, which will require them to meet a more exacting legal standard. As a practical matter, some cross-cutting authority will usually be available, thus rendering apparent privacy protections vaporous, but depending on the nature and posture of the specific investigation—and often with no reference to any genuine privacy interest—the standards will sometimes leap higher. The result is a peculiar environment in which privacy protections mostly do not mean what they seem to say in the context of the higher-stakes government investigations, except when then suddenly do. It is an environment that raises an important structural question: What is the point of these ostensibly tough protections for data if prosecutors can generally—but not always—circumvent them when it actually matters?

A second axis of irrationality is that many statutes provide for wildly differing means of acquiring the same or similar data. Take the rules governing court-ordered disclosures in criminal cases. As noted above, collection law generally authorizes prosecutors to get information about their targets by applying for a court order, which in turn compels a third party to divulge the requested materials. Law enforcement may choose not to use these procedures when a grand jury subpoena is available to them, but when, for one reason or another, a subpoena will not do, the procedures often require notice to the affected individual, and sometimes even vest the target with the ability to contest the order in court. The Video Privacy Protection Act, the Cable Act, and the Electronic Communications Privacy Act all establish some iteration of this kind of process. And the three laws all require the government to make different legal showings before a judge may order the production of the data they cover than do laws covering data of comparable sensitivity.

Thus, for example, a court may command Comcast to disclose your cable video viewing history only if the government presents “clear and convincing evidence” that you are “reasonably suspected of engaging in criminal activity” and that information about your cable account “would be material evidence in the case.”⁵⁰ At the same time, if prosecutors want to compel disclosure from Netflix—arguably a “video tape service provider” and thus subject to the VPPA—they must instead

⁵⁰47 U.S.C. § 551(h)(1).

show “probable cause to believe” that your particular rentals are “relevant to a legitimate law enforcement inquiry.”⁵¹

Neither of these phrases is a model of clarity, even by the forgiving standards of contemporary legalese. Precisely what is “clear and convincing evidence” of a “reasonable suspicion” and is that a looser or more rigorous standard than “probable cause” of “relevance”? What’s more, the differences between them is quite inexplicable. There is no good reason why “clear and convincing evidence”—a quantum of proof lying somewhere between the “preponderance of the evidence” required for civil liability, and the “beyond a reasonable doubt” required for a criminal conviction—should be necessary in order to obtain a court order in the cable records context, while probable cause reigns with respect to video records. Of course, there may not be much of difference between these differing standards in practice; perhaps the procedure and required proof are, in practice, roughly the same whenever prosecutors ask a judge to order the production of video rentals or cable information. But if we want consistent standards across media, it would make sense to have consistent statutory language. The courts, after all, generally take Congress’s distinct word choices to mean something. Meanwhile, no specific law regulates the acquisition of purchase or rental records for other media. Investigators can simply ask for that your book or music purchases.

The law’s treatment of an email, as we have already suggested, provides another good example of this point. Hypothesize a very sensitive personal email sent you by your sister. If you are a Gmail or other cloud-based email user, then the government cannot discover the message’s contents within the first 180 days of its life without obtaining a warrant—unless, that is, you open it. According to the Department of Justice, an email in the cloud that has been accessed by the user is reachable according to the same, less demanding standard that governs emails at least 181 days old.⁵² By contrast, if you download the email to your personal computer, then the 180-day time clock disappears entirely, the Fourth Amendment is triggered, and the government must obtain a search warrant before collecting, no matter how long the message has resided on your machine. The degree of privacy protection your email receives is conditioned by a variety of different factors—some rational, some utterly archaic.

Compare that to the protection given to snail mail, which involves directly comparable physical data entrusted for delivery by a third party. If your sister, instead of emailing you this sensitive note, puts it in an envelope and in the mail, then the State cannot intercept it in transit and read it unless it first obtains a search

⁵¹18 U.S.C. § 2710(b)(3).

⁵²The government’s argument regarding opened, cloud-based email has persuaded some district courts but apparently has not been endorsed—or specifically rejected—by any appellate court. *See, e.g., United States v. Weaver* 636 F.Supp.2d 769, 769-70 (C.D. Ill. 2009) (ordering disclosure of emails less than 181 days old and residing on defendant’s hotmail account, pursuant to trial subpoena).

warrant.⁵³ The legal standard applicable to search warrants—probable cause—likewise comes into play if she calls you to discuss the matter on the phone, and the police wish to listen in with a wiretap.⁵⁴ In a wide range of areas, we do not treat similar data similarly.

The flip side of this oddity is that the law overprotects some less sensitive data, while underprotecting other more sensitive materials. Everyone accepts that some personal information deserves more legal protection than other information. Not all information is equally valuable—in terms of privacy, personal security, or investigative power—and any rational set of rules thus must treat some kinds of information more delicately than others. From a systemic perspective, then, one wishes to see a hierarchy in which more sensitive material receives greater protection while less sensitive material receives lesser protection. At a minimum, one would like to see an *effort* in that direction. Yet our current crop of collection authorities does not reflect any such hierarchy. It reflects, rather, a weird hodgepodge of responses to discrete policy problems or, sometimes, discrete incidents.

The classic example of this point is the relatively severe hoops through which (in the absence of a subpoena) authorities have to jump to find out what videos we rent and the cable television programs we watch. That quirk is in part a product of Robert Bork's unsuccessful nomination to the United States Supreme Court. Bork's rejection by the Senate, and the debate over its impact on judicial confirmation politics, are both famous. Less well known outside of privacy circles is the legislation enacted in response to the coverage of Bork's failed candidacy. During his nomination's consideration—and in response to Bork's controversial repudiation of a constitutional right to privacy—a journalist named Michael Dolan asked the video store he and the judge both patronized to provide him with a list of videos that Bork had rented. Because no law forbade it, the store gave Dolan the list, and the *Washington City Paper* ran Dolan's article, which noted a few of Bork's past rentals and speculated about their significance.⁵⁵ Appalled at the invasion of Bork's privacy, and recognizing that legislators' own entertainment interests might be similarly aired, Congress passed the Video Privacy Protection Act (the "VPPA") in 1987.

On its face, the VPPA goes a long way to keeping video rental records out of the state's hands. As discussed above, it prohibits video businesses from divulging the records of their members' past rentals. Unless presented with a warrant, a court order, or a grand jury subpoena, a video store cannot disclose rental lists like

⁵³See *Ex Parte Jackson*, 97 U.S. 727, 733 (1877) ("The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, ... as is required when papers are subjected to search in one's own household.").

⁵⁴18 U.S.C. § 2518(3)(a).

⁵⁵Michael Dolan, "The Bork Tapes," *Washington City Paper* (Sept. 25-Oct. 1, 1987).

Bork's to investigators, and may face civil liability if it does.⁵⁶ Courts, moreover, will not order the disclosure of viewing histories unless civil litigants or law enforcement can meet especially rigorous legal standards; before a judge will intervene, the latter must show probable cause that the viewing records are relevant to a criminal investigation. And finally, video rental information acquired in violation of the VPPA cannot be introduced into evidence in subsequent legal proceedings. The VPPA hints at the influence of the Cable TV Privacy Act, which was enacted three years earlier; much like the VPPA, it keeps cable customers' programming choices away from the government, unless it can obtain a legally demanding court order.⁵⁷

Yet as we have noted, comparable classes of information come nowhere close to enjoying the same privileged status as video and cable records. By means of a trial subpoena, prosecutors can simply request, and courts will order, Barnes & Noble to provide authorities with receipts documenting your purchases of a hardback copy of "Doctor Zhivago" without the government's first having to meet the tougher requirements that would have been implicated if you had elected to stream the movie adaptation of Pasternak's novel or to watch the film on HBO.⁵⁸ And no law forbids vendors in most media from simply turning over records on law enforcement request. A great deal of media is now sold online, and the larger e-businesses trade both in music and video services, on-demand as well as mail-order. Consequently, iTunes and its customers must navigate at least two quite-disparate third-party disclosure regimes depending on what material a user has bought. Which one applies will turn on whether a customer downloads a song or streams an online movie, with the record of the song purchase receiving far less in

⁵⁶Courts have disagreed about precisely who is subject to liability under the VPPA. Its text authorizes aggrieved individuals to bring suit against any "person;" the debate turns on whether that word extends to defendants other than video service providers. Compare *Dirkes v. Borough of Runnemede Police Department and Lieutenant Emil P. Busko*, 936 F. Supp. 235, 239-40 (D.N.J. 1996) and *Camfield v. City of Oklahoma City*, 248 F.3d 1214, 1217-1218 (10th Cir. 2001) (approving suits against law enforcement officers for allegedly receiving personal information derived from violations of the VPPA) with *Daniel v. Cantrell*, 375 F.3d 377 (6th Cir. 2004) (rejecting Dirkes analysis and stating that only video service providers may violate § 2710(b)).

⁵⁷47 U.S.C. § 551(c)(2)(D), (h).

⁵⁸FED. R. CRIM. P. 17(c). The lack of statutory protection for book purchase records is especially ironic given that Congress thoroughly considered the need for such protection, during the VPPA's drafting. The statute's legislative history refers to this statement by Representative Al McCandless, the sponsor of the first video privacy bill:

There's a gut feeling that people ought to be able to *read books* and watch films without the whole world knowing. *Books and films* are the intellectual vitamins that fuel the growth of individual thought. The whole process of intellectual growth is one of privacy--of quiet, and reflection. *This intimate process should be protected from the disruptive intrusion of a roving eye.*

S. Rep. 100-599 at 7 (1988). (emphasis added). Consistent with McCandless' testimony, the Senate's Judiciary Committee "recogniz[ed] that there is a close tie between what one views and what one reads." *Id.* at 8. However, the Committee was unable to resolve how to apply a proposed restriction on the disclosure of library records to law enforcement, *Id.* Thus, as enacted, the VPPA's coverage was limited to records pertaining to a customer's video rentals.

the way of privacy safeguards.

This makes no sense. It is an artifact of a relatively recent time when different distributors handled different types of media, when the lines between rental and purchase were more pronounced than they are today, and when the modes of transmission of those media still tended to involve the transportation of physical objects. There is no good reason now in a digital world to treat media purchase and rental records with a kind of regulatory apartheid. The individual's privacy interest in his or her video viewing habits is no greater or lesser than the comparable interest in his or her reading lists, music purchases, or cable records. Whether it is generally more sensitive than information reflecting whom he or she talks to or how he or she uses a credit card seems to depend entirely on what sort of videos he or she rents versus in whose hands he or she places the credit card. To the person who rents a lot of pornography but pays for it only in cash, a system that protects videos but not credit card records will seem the height of sense. On the other hand, to the person who rents anodyne romantic comedies but funds a secret habit of playing online poker with her Visa card, it will seem very backward indeed.

The mismatch between data sensitivity and the degree of protection it receives is most evident in the comparatively lenient standards for investigative access to education records⁵⁹ and health information relative to the standards just discussed.⁶⁰ Disclosure of such data can mean, among other things, revelation of past punishment for dishonesty or other misbehavior, or treatment for severe or embarrassing health problems. The likelihood that disclosure will lead to humiliation or material harm seems manifestly higher in the educational context and, particularly, in the health context than in the context of consumption of some—but not all—media. And yet the safeguards attached to education and health data are not at all stringent, despite the intimate character of the information at issue.

This is especially true with respect to education records. Nothing in federal law limits government acquisition of educational records. Indeed, nothing in federal law makes it illegal for schools to disseminate educational records to anyone. Congress, rather, conditioned the receipt of funding from the Department of Education on a school's compliance with the privacy principles codified in the Family Educational Rights and Privacy Act ("FERPA").⁶¹ In other words, unlike video businesses, cable or telecommunications companies or health care providers, educational institutions can at least in theory choose not to obey federal privacy

⁵⁹20 U.S.C. § 1232g(4)(A) (defining "education records," with certain exceptions, as "those records, files, documents, and other materials . . . which contain information directly related to a student," and which "are maintained by an educational agency or institution or by a person acting for such agency or institution.").

⁶⁰45 C.F.R. § 160.103 (protected health information includes all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form).

⁶¹20 U.S.C. § 1232g(b).

law. And for schools that receive federal educational grants, the lone restriction is lenient: the Secretary of Education will withhold the Department's money if a school has a "policy or practice" of disclosing education records in violation of federal privacy rules—but not if a school divulges information in one or a few discrete cases.⁶² (By contrast, aggrieved individuals can sue cable companies, video businesses, and financial institutions whenever their personal information is wrongfully disclosed.) Unlike the cable, video, and electronic communications laws, FERPA lacks even a nominally-demanding provision for court orders in criminal cases.

The Health Insurance Portability and Accountability Act ("HIPPA") and its implementing regulations likewise do not outline any particular standard that prosecutors must meet before obtaining a court order compelling the disclosure of health information. Both FERPA and HIPPA employ the same broad exceptions that govern other corners of collection law. Prosecutors can send a grand jury subpoena to a health care provider or school, for example.⁶³ And with respect to educational institutions, on a showing of good cause, the government also can prevent a school from telling the affected student about the subpoena.⁶⁴ National security provisions also allow for easy collection of health and educational information, and understandably without notice to the affected person. Entities covered by HIPAA may disclose protected health information to authorized federal intelligence personnel without any prior showing by the government. Likewise, if the executive branch merely certifies—not proves—that there are "specific and articulable facts giving reason to believe that educational records are likely to contain" information relevant to a terrorism offense, then a federal judge *must* enter an *ex parte* order compelling the college to hand over the records.⁶⁵

Towards Rationalization

Before discussing strategies for rationalizing this sprawling patchwork of laws, we should pause to address a question on which many readers may reasonably get hung up: Why bother to rationalize it? The system, a defender—or even a merely complacent observer—might plausibly argue, achieves a kind of rough balance. Government can generally get access to information when it needs it, but it does not get presumptive access—thus ensuring both a baseline level of privacy for the public and the satisfaction of investigative needs. While it's not a pretty system and certainly not one that anybody would find conceptually satisfying, its ambiguities reflect genuine societal uncertainty as to the proper contours of a collection system.

⁶²20 U.S.C. § 1232g(b)(1); *see also Gonzaga University v. Doe*, 536 U.S. 273, 288 (2002) ("FERPA's nondisclosure provisions further speak only in terms of institutional policy and practice, not individual instances of disclosure.").

⁶³45 C.F.R. § 164.512(f)(1)(ii)(B); 20 § 1232g(b)(1)(J)(i).

⁶⁴20 § 1232g(b)(1)(J)(i).

⁶⁵20 § 1232g(j)(2)(A)-(B), (j)(1)(A).

We want robust, speedy unencumbered investigations and we want strong privacy protections. We want the government to connect the dots about terrorists, but we emphatically want our own dots left unconnected. Our collection system, in its incoherence, reflects these conflicting claims. And rationalization will force us to select winners and losers where we now have delicate, if messy, compromises.

This objection has two major problems. The first is that these elaborate compromises actually serve well none of the many interests at stake in a collection system. For government, it creates a system of enormous complexity. It's a system that expects investigators to act differently depending not merely on the type of information and the type of investigation in question but based on such factors as the age of the information, the location of the information, the location of the target, the identity of the investigator, and the citizenship of the target. As Kris noted in the context of the FISA Amendments Act in the language quoted above, this complexity itself is dangerous both to investigative needs and to privacy. Businesses, for their part, suffer both from the system's complexity and from the ultimate weakness of the protections. Typically, the third-party in whose hands individual data rests is a business and the data are often transactional records recorded automatically. Businesses thus face daily a messy dance between the flood of government demands for this information and the laws that prohibit their disclosure of certain information. Google alone in the first half of 2010 received more than 4,000 requests or demands from authorities in the United States for user data, and this figure does not include any NSLs or similar requests that the company may have received in that time frame.⁶⁶ As a practical matter, industry will almost always have to produce at least some of the requested material to government investigators. But the system's complexity requires work to verify that obligation and to see where it may not apply or where disclosure obligations may be narrower than investigative demands—not to mention to see where legal restrictions on disclosure may convey liability if breached. The system's competing obligations of protection of data and disclosure of data can operate as a pincer against the businesses that act as custodians of people's records.

For civil libertarians, meanwhile, the current system is a kind of a ruse. As we have seen, the protections that it offers often appear far more robust than their actual operation. Strong protections in one context merely incentivize the acquisition of information outside of that context—the use of those instruments that require lesser showings or involve lesser bureaucratic hassles. In reality, for most data, the government gets access rather easily at the end of the day, and the system operates less by imposing substantive roadblocks than by requiring the

⁶⁶See "Transparency Report: Government Requests," available at <http://www.google.com/transparencyreport/governmentrequests/> (last visited on Dec. 20, 2010). Because NSLs preclude recipients from acknowledging the NSLs' very existence, Google naturally has not released data on any NSLs it may have received. See "Government Requests FAQ," available at <http://www.google.com/transparencyreport/faq.html#governmentrequestsfaq> (noting that publicly released data on government information requests are not comprehensive) (last visited on Dec. 20, 2010).

filing of certain paperwork and the making of certain representations. This creates an illusion of privacy, but the illusion is thin. And that illusion, that obscurity, is inimical to civil liberties. We should not want, after all, apparently strong but ultimately farcical privacy protections. We should, rather, want collection laws that are clear in what they protect and what access they permit. In short, the system's lack of coherence serves less to create a rough kind of balance than to create obscurity, complexity and illusion.

Second, forcing us to select winners and losers is actually a good thing, not a bad thing. The proliferation of mosaic data makes it simply inevitable that we make choices about when government gets access to that data and under what circumstances. We cannot avoid this. Refusing to engage the subject systematically does not actually produce a messy compromise of the sort that may be defensible. It still produces winners and losers; it just doesn't do so deliberately. The process of rationalization is a process of making choices overtly and carefully. It is a process of identifying the principles that should govern the acquisition and investigative uses of personal data by government and applying those principles in a fashion that makes it clear whom they benefit and whom they hurt, when, and why.

There is, to be sure, a limit to how simple the system can become—and none of what follows is meant to argue for ignoring important distinctions. Some of the system's complexity, after all, reflects genuinely significant distinctions between the acquisition in different circumstances of different data types. Employer-provided email is not the same as personal email; mass acquisitions of huge quantities of data is not the same as acquisition of individual pieces of data for specific investigative and forensic purposes. A system of perfect consistency would necessarily obviate such distinctions, and taking account of them will create complexity. The task of rationalization is one not of eliminating meaningful and valuable distinctions but of eliminating distinctions that add only unpredictability and obscurity.

This type of rationalization requires two things not evident in the modern history of our policymaking in this area: It requires a coherent theory of government access to mosaic data in the hands of third parties, and it requires that we make decisions about how to protect that data not in the abstract but in relation to how we wish to and do, in fact, protect other similar and dissimilar data. It will not do to say as an abstract matter that data of Type A is personal and should be kept private and impose a high standard for its acquisition without reference to the fact that data of Type B is, in most people's view, *more* sensitive yet receives no comparable protection. Nor will it do to create a rule for data of Type A so stringent that it becomes a nullity because some broad stopgap will ensure that we never have to submit to the standard we create. Our law should proceed from a simple theory of what sort of data we want to protect from government acquisition, when, and how. The rationalization of collection authorities should reflect an attempt to apply that theory as broadly and evenly as we can, taking into

account the unique policy issues that different data types may present. We should not be making policy individually for, say, cable records, medical records, geolocation records, and stored communications records unless something unique to these data types requires it. We should, rather, think about policy for government access to the mosaic's many tiles.

One can, of course, rationalize and simplify in any number of directions. Policymakers could take the view, for example, that the system's basic flaw is that the burdens it places on the government are, in many instances, insufficiently stringent, and they could rationalize and simplify the system by raising the floor to some uniform level. Conversely, they could take the view that the basic problem is that needless and largely ineffective civil liberties protections sometimes impede useful government data access and conclude that the appropriate response is to strip these away and leave a uniform standard of access based on minimal showings and procedures. A more complicated approach would be to attempt to maintain a layered, textured set of authorities, but to try to harmonize their protections with society's sense of the relative importance of different types of records.

The approach to rationalization we outline here partakes of all three of these strategies. In our view, current law protects some records insufficiently, protects others—at least in some situations—too rigorously, and as a consequence does not reflect any kind of societal judgment about the relative importance of different types of mosaic data. The logical approach, therefore, is to lower some barriers, raise others, and calibrate protections *with reference to one another*. The goal is a system that has three key features.

First, it should calibrate data protections in rough proportion to the sensitivity of the different types of data. Second, it should not make privacy protection a derivative function of the nature of the specific technology the user chooses. A rational system would not give less protection to the contents of email communications than it does to the contents of physical mail or telephone communications, nor would it give email addressing information *more protection* than it gives to mail or telephone communications.⁶⁷ It would, rather, be technology-neutral. Third, it should not provide multiple, duplicative authorities for the acquisition of the same data but, rather, should reflect parsimony; a given investigative need should give rise to as few options as possible for acquisition. The appropriate option for government collection in any given situation should be obvious both to investigators and to the public.

⁶⁷Compare 18 U.S.C. §§ 3122 (b)(2), 3123(a)(1)-(2) (courts will order the use of a pen register or trap-and-trace device, if the government certifies that information likely to be obtained will be relevant to an ongoing criminal investigation) with 18 U.S.C. § 2703(d) (court will only order the disclosure of the non-content addressing information concerning emails if the government makes a showing of “specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation”).

At the end of the FISA modernization paper we quoted at the outset, Kris teased out a possible rationalization of collection authorities in national security investigations:

For the long run, at least, it is possible to imagine a simpler world in which national security investigations are governed by only two major collection statutes. The first statute would apply more or less as broadly as a grand jury subpoena, perhaps also including surveillance currently conducted by using pen registers and trap-and-trace devices. That could replace the various national security letter statutes, the FISA pen/trap provisions, the mail cover regulations, and perhaps the section of the Patriot Act that permits acquisition of business records. All of those laws allow the government investigators to acquire certain information, but they do not authorize full-blown searches or wiretapping. . . . It is possible to imagine one consolidated statute to replace some or all of these provisions, setting up a simpler, clearer system for regulating investigative techniques other than wiretapping and searches in a national security investigation.

The second major statute would govern any acquisition of information for which a warrant would be required if undertaken for law enforcement purposes in the United States. If the government has to go before a judge and demonstrate probable cause in a criminal investigation, it would have to do so in a national security investigation. For example, the government would use the second statute to enter and search a home or office, to conduct a wiretap, or to place a hidden microphone.⁶⁸

Notice how Kris's proposal addresses all three of the features we have associated with a more rational system: It attempts to treat similar data similarly. It makes the system more technology independent. And it injects parsimony and simplicity into what is now comparatively chaotic and disorganized.

The simplification we imagine here follows a similar arc, though it is both more and less ambitious than Kris'. It is more ambitious in the sense that it incorporates criminal acquisition authorities, as well as national security authorities, and actually proposes changes to the evidentiary thresholds the government must meet to acquire different categories of data. It is less ambitious in the sense that it does not encompass wiretapping or physical search authorities, merely the acquisition of mosaic data held in the hands of third parties. It proposes a "simpler world," as Kris might put it, to govern the acquisition of those many categories of data for criminal or national security purposes.

It no doubt oversimplifies matters to say that all personal mosaic data in the hands of third parties can be divided into one of three categories—but it doesn't

⁶⁸ David S. Kris, "Modernizing the Foreign Surveillance Act," in *LEGISLATING THE WAR ON TERROR: AN AGENDA FOR REFORM* 234-235 (2009).

oversimplify matters all that much. And as the system is today at no conceivable risk of becoming so simple as to lack nuance, we propose three and only three categories of data as a working model for reform.

First, there are one's personal records: the contents of communications of ever-proliferating types (emails, text messages, instant messages, and the like) and the many documents, financial data, photographs, and other files that we now store in cloud computing servers, rather than in our desks and on our personal hard disks. These are, broadly speaking, dramatically under-protected under current law. The first step towards rationalization, therefore, is to *raise the floor for acquisition of material that directly parallels material that is traditionally stored in one's house or office and is there protected by the Fourth Amendment's warrant requirement.*

Second, there are transactional and other business records that are not one's own records but, rather, someone else's records of one's interactions with and uses of their services: credit card and bank logs, telephone and email addressing and routing information, purchase and rental histories, library records, and EZ-Pass toll booth data, to name just a few. These records, as we have shown, have varying degrees of privacy protection associated with them in the absence of a grand jury subpoena—almost all of which prove fictitious when a subpoena materializes under a mere relevance standard and some of which are collected in bulk for security reasons. Meanwhile, much data of this type gets no protection at all; it can simply be produced on request. In our view, a baseline level of protection ought to apply to transactional data much more broadly than it does, but the fictitious and often extravagant protections ought to be stripped away in both criminal and national security investigations. *All non-public routine transactional and business records that are reflective of individual behavior and stored in electronic systems of records ought to be presumptively shielded from government access yet acquirable easily and without a heightened showing either in the investigative context or in the context of security-oriented bulk acquisition. In the investigative context, they should be produced under a simple relevance standard whether or not a grand jury is sitting.* Broadly speaking, we should require a simple and uniform order to acquire this sort of material and stop kidding ourselves that the protection against its abuse will lie in legal restrictions on government acquisition and focus instead on restrictions on and regulations of the use and dissemination of such data after acquisition. In the non-investigative security context, we should have a high tolerance for statutes and policies that authorize bulk collection for data-mining purposes, so long as the collection is necessary for an essential security function.

Third, there exist specific categories of transactional data that, either individually or when aggregated, present such a vivid portrait of a person that their acquisition is unusually sensitive. The paradigmatic case of this type of material involves health care data. Scholars and advocates argue about what other data types are comparably sensitive, and we don't mean to resolve that dispute here. But *these types of transactional data should be subject, in our view, to special designation by Congress and, following that, acquisition under an intermediate standard*

with prior judicial authorization whether or not a grand jury is sitting.

Let's consider each of these categories in turn.

Personal Records

The Fourth Amendment protects material stored in people's homes and offices, storage lockers, on their own computers, and in their cars.⁶⁹ As such, in the physical world, it protects one's stored records and correspondence, files, photographs, and videos. It broadly speaking protects in the physical world all of the sorts of records one keeps in one's desk and the sorts of media—the books, the music, the pornography, the home movies—that one keeps in one's personal spaces. It also protects one's communications in transit: The government cannot open your mail without a warrant and it can't intercept your telephone communications without a warrant either.⁷⁰ In other words, in the physical world, your communications and your stored records are unambiguously within the ambit of the Fourth Amendment unless you behave like an idiot. If the government wants to seize this material in real time, it needs a warrant issued in advance by a judge on a showing of “probable cause.” If authorities do not want to meet this evidentiary threshold, they can issue a subpoena for the material (if the material is tangible) on an assertion of relevance, but they have to issue the subpoena to *the target of the surveillance*. This gives the target an opportunity to contest the collection. Authorities cannot end-run this opportunity by, for example, issuing a subpoena to the postal service to inspect the contents of someone's mail or issuing a subpoena to the person's landlord to seize his papers—though the landlord does own the person's residence.

Exactly how the Fourth Amendment applies in cyberspace is a complicated question, though as we have seen, the statutory collection authorities governing materials online that are analogous to materials protected in the physical world by the Fourth Amendment are far more permissive. One school of thought treats this as a natural corollary of the third party doctrine, under which one generally cannot assert Fourth Amendment protection to shield material voluntarily entrusted to someone else.⁷¹ By contrast, an emerging school of thought seeks to translate the protections of the Fourth Amendment into the cyber-sphere. In a recent article, Fourth Amendment scholar Orin Kerr argues that the Fourth Amendment should

⁶⁹*United States v. Turner*, 169 F.3d 84 (1st Cir. 1999) (suppressing files obtained during warrantless search of defendant's computer, when defendant's consent did not extend to the computer);

⁷⁰*See Ex Parte Jackson*, 97 U.S. 727, 733 (1877) (“The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, ... as is required when papers are subjected to search in one's own household.”); *Katz v. United States*, 389 U.S. 347, 353 (1967) (applying Fourth Amendment protection to defendant's telephone call, placed from an enclosed telephone booth).

⁷¹*United States v. Miller*, 425 U.S. 435, 443 (1976); *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)

be understood through a lens of “technology neutrality,” which “assumes that the degree of privacy the Fourth Amendment extends to the Internet should try to match the degree of privacy protection that the Fourth Amendment provides in the physical world. That is, courts should try to apply the Fourth Amendment in the new environment in ways that roughly replicate the role of the Fourth Amendment in the traditional physical setting.” The right analog for the physical world, where the Fourth Amendment generally requires a warrant to search inside a private space while not requiring a warrant for surveillance outside of one, Kerr argues, is the distinction between the contents of Internet communications and other data about those communications: “the contents of online communications ordinarily should receive Fourth Amendment protection but th[e] non-content information should not be protected. This approach accurately translates the traditional physical distinction between invasion into enclosed spaces and evidence collection in public.”⁷²

Whether Kerr’s theory, or something close to it, eventually catches on as constitutional law, it represents extraordinarily sound public policy to which Congress ought to conform our collection regime. The Fourth Amendment, after all, protects our physical spaces in part so that it may protect the tangible property within them. When one receives communications by email, instead of snail mail, and stores that email on a remote server, instead of in a physical filing cabinet, one is still engaged in the same activity—still deserving of the same shield. One is reading one’s mail. One may, in fact, quite literally still be doing that same activity in the same room of the same house. To fail to protect emails and remotely stored personal records as robustly as the Fourth Amendment requires for communications and records in the physical world involves a substantial net loss of privacy from the baseline the Fourth Amendment was designed to ensure.⁷³

The defining feature of this class of records is that it involves the user’s material held by the third party—*her* documents, communications, files, and the like—which directly parallel materials for which she reasonably expects protection in the physical world. It is material entrusted by the user to the third party for purposes of transmission or storage, not material generated by the third party to record interactions with the user. As such, it is, broadly speaking, the sort of material we all used to store in our desks and on our shelves and walls. That the

⁷²Orin S. Kerr, “Applying the Fourth Amendment to the Internet: A General Approach,” 62 STAN. L. REV. 1005, 1007-1008 (2010). Just before this paper’s publication, the United States Court of Appeals for the Sixth Circuit effectively adopted Kerr’s approach. The Court held that the Fourth Amendment’s warrant procedure applies to the contents of third-party e-mails which are stored by electronic service providers. *United States v. Warshak*, No. 08-3997, 2010 WL 5071766 (6th Cir. Dec. 14, 2010).

⁷³In this sense, our recommendations are consistent with those advocated by Digital Due Process, a non-profit organization advocating for reform of the Electronic Communications Privacy Act and related statutes. See generally J. Beckwith Burr, the Electronic Communications Privacy Act of 1986: Principles for Reform,” available at http://www.digitaldueprocess.org/files/DDP_Burr_Memo.pdf (last visited on Dec. 20, 2010).

Fourth Amendment’s framers could never have imagined that such material might be stored in the cloud does not make it remotely less sensitive or deserving of protection. We take no position here as to how judges should adapt Fourth Amendment law to this change. But it presents a clear task for Congress if it means the law to maintain the values that the amendment was crafted to embody.

The rule for this class of materials should directly parallel the rule in the physical world: To get one’s personal records in real time from service providers, authorities should need a warrant issued on a showing of probable cause by a judge. In a national security investigation involving a U.S. person or someone reasonably believed to be in the United States, that judge would sit on the FISA Court; in a criminal probe, that judge would be at the local federal district court.⁷⁴ Conversely, if the government chooses to use a subpoena instead of a warrant, it can issue a subpoena *to the surveillance target*—an option that for reasons of secrecy cannot be available in the national security arena. An investigator should not, however, be permitted to use the instrumentality and suppressed standards of a subpoena to win real-time access to the contents of personal records.

This rule should cover all non-public Internet communications, and all documents, files, and personal data that *an individual* stores in the cloud. It should not, however, cover employer email accounts, which the individual does not own or control. Law enforcement should be able to obtain access here by issuing a subpoena to the employer, not the individual. And it should not cover the cloud-stored materials or communications content of non-U.S. persons reasonably believed to be overseas.⁷⁵

Routine Transactional and Business Records

If the acquisition standard for the contents of personal records is often too low, the rules for routine transactional records have a different problem: The proliferation of competing standards tends to mask how low it really is—and properly needs to be—when things really count. Even as Congress establishes a uniform floor for content acquisition, therefore, it should also strip away the many competing standards for transactional records and make clear that in all criminal and national security investigations, the government does not have presumptive access on request to routine transactional data and business records but may obtain access on a simple administrative assertion of relevance to an investigation—an assertion that sees judicial review if and only if the holder of the data challenges it.

⁷⁴The nature of the probable cause showing would differ too between different types of investigations. In a criminal investigation, the showing would involve probable cause of a crime, whereas in a national security investigation, it would involve probable cause of agency of a foreign power.

⁷⁵In other words, it should not upset the fundamental balance reflected in the FISA Amendments Act, in which the intelligence community is entitled to collect material in bulk related to the activities of non-U.S. persons not believed to be in the country without specific showings relative to them.

This rule should govern whether or not a grand jury is sitting and irrespective of whether the investigation in question is criminal in nature or concerns national security. It should replace the many different rules that now govern acquisition of these records—the national security letter statutes, the FISA business records statute, and the data-specific rules like the video, cable, and credit card record laws. And it should apply far more broadly than current rules do—not just to video but to all media purchases and rentals, for example. Broadly speaking, mosaic data involving non-public records of individual interactions with third-party businesses should be shielded from production to investigators in the absence of process, but that process should be far easier and more streamlined than are many of the competing systems at play today. We should replace the vast bulk of them with a single acquisition authority that parallels the production of material reachable by grand jury subpoena. This instrument should be both bureaucratically and substantively easy to issue—roughly like the current NSL, only with the secrecy associated with the NSL only present in national security investigations or when necessary to protect lives.

As a practical matter, this change would affect privacy in uneven ways. For mosaic data currently unprotected by any law, it would have the effect of requiring that the government use some legal process to acquire it. In other words, much more data would be presumptively out of the government’s reach than is now. On the other hand, the process associated with acquisition would be minimal and easy—and critically, it would be even across data types. Acquisition of credit card records, phone records, book purchase records, video records, and toll-booth records would all proceed according to the same simple, clear rules under more or less the same standard as compulsory production proceeds now.

Nearly all of this material, we stress, is acquirable under subpoena-like procedures already. As we have seen, the apparently strong privacy protections for some data categories are largely chimerical. The rules and procedures differ between the different authorities, but at the end of the day, the government almost always gets transactional data that it deems relevant to its investigations, for the simple reason that some cross-cutting authority will generally be available. Clarifying that this is the rule makes good housekeeping sense, and it would be enormously clarifying for the public. Harmonizing the procedures and standards between data types makes sense as well. There is no point in having laws suggesting that the government needs probable cause to access video records when it doesn’t. There is no point either in having a bewildering array of authorities to access telephone and email addressing information under authorities that differ somewhat in substance and procedure but largely amount to the same thing. Acquisition should, rather, all flow from the same principle and thus the same authority. The structure should be the administrative subpoena, and the standard should be relevance.

This point has an important corollary in the context of bulk collection of mosaic data for security purposes—programs like the routine collection of passenger

reservation data from airlines and bank transfer data from SWIFT. The corollary is that we should have a broad tolerance for bulk acquisition of routine transactional data where the acquisition and analysis is necessary for an essential security function. These programs have generated extraordinary controversy, and they don't fit neatly into the scheme we outline here. After all, the purpose of collection is more of a generalized security and intelligence function than the supposed relevance of any individual bit of data to any particular investigation. And while sometimes, as with SWIFT, the collection takes place pursuant to subpoena, the animating feature of the program is not the data's relevance to any one investigative inquiry. Yet if we accept that routine transactional data is presumptively shielded from government in the absence of cause for collection but that relevance to an investigation is adequate cause, it follows that relevance to an essential security function is also adequate cause. We don't propose that such a rule should give rise to its own general authority to collect, a principle that could swallow all restrictions on government access. Rather, such bulk collections should remain *sui generis* policy judgments, authorized by their own statutes and executive orders. Our point, rather, is that this approach offers a useful clarifying lens through which to evaluate the validity of such collection efforts and the controversy that tends to surround them. Put simply, we should view collection that is limited to routine transactional data (with respect to U.S. persons) and reasonably related to an essential security function as presumptively valid.

This is not to say that there should exist no privacy protections for business and transactional records, just that we should not rely on restrictions on acquisition for that protection. We should, rather, look to restrictions on use of data once acquired, to administrative and criminal punishment for abuses and mishandling of materials, and to audits and monitoring of data by inspectors general and other internal accountability mechanisms.

These data are, it bears emphasis, quite different from the materials in the first category. They are not the user's personal records, stored by the third party. They are, rather, the *third party's records* about the user. They are not the phone call you make or the email you sent, but the addressing information regarding whom you contacted and when. They are not the contents of the off-site backup for your desktop computer, just the credit card record that you paid \$40 to the backup company. While particularly when aggregated, they can describe a rich portrait of your life, they are the sort of material that has never been protected and always been reachable with a subpoena. With respect to this type of data, the loss of privacy we are experiencing in modern society flows not from an erosion of the scope and reach of the Fourth Amendment but from the proliferation of digital fingerprints modern people leave in their day-to-day lives. For nearly all such transactional and business records, in contrast to users' personal records, the absence of Fourth Amendment protection reflects a coherent judgment that investigative and security interests in this material simply outweighs user privacy interests in it. The system's irrationality in this area lies not in this judgment but in the erratic and inconsistent application of that judgment and the laws that seem to

obscure it.

Especially Sensitive Transactional and Business Records

If one valued simplicity over everything else in a system of collection authorities, one could simply stop there. The trouble is that there are certain categories of transactional and business data that are inordinately more sensitive than others. The prototypical example is health records. The prescriptions filled for you at the pharmacy and the records of the medical treatment that generated those prescriptions involve an intimacy of a different order of magnitude than your credit card records—even those credit card records of the transaction with the pharmacy and the clinic that wrote the prescriptions. Other types of data, either individually or in aggregation, present similar anxieties. Some scholars and courts have argued, for example, that geolocation data from cell phones are similarly sensitive and should require a warrant.⁷⁶ And one could imagine an argument that a pen-register or trap-and-trace device order should receive, as it gets now, prior judicial consideration—though the current substantive standard under which such orders issue is mere relevance. While people will disagree about which specific types of data require some kind of heightened evidentiary burden for production, most scholars and commentators seem to agree that not all transactional data are created equal.

Without defining precisely which data belong in this category, let us therefore propose the existence of a third category of mosaic data: transactional and business records of a sensitivity sufficient to require something more from the government than a mere subpoena. For this category, we could imagine a standard and procedure similar to those which the Stored Communications Act applies to the non-content records concerning electronic communications: a warrant-like production order based on “specific and articulable facts that there are reasonable grounds to believe that the [sought items] are relevant and material to an ongoing criminal investigation.”⁷⁷ The current rule for FISA business records also offers a model here, requiring “reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation.”⁷⁸ In both cases, production requires, as with a warrant, judicial pre-approval, and the standard is more

⁷⁶Compare *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010) (rejecting warrantless, 24-hour a day surveillance of defendant’s physical location, derived from tracking instrument placed on defendant’s vehicle) with *United States v. Pineda-Moreno*, 591 F.3d 1212 (9th Cir. 2010) (affirming guilty plea, and finding no constitutional violation, when police entered curtilage of the defendant’s home, and affixed a tracking device to the underside of his car); see also “Our Principles,” available at <http://www.digitaldueprocess.org/index.cfm?objectid=99629E40-2551-11DF-8E02000C296BA163> (last visited on Dec. 10, 2010) (arguing that government should only be allowed to require communications companies to provide “location information regarding a mobile communications device [upon presentation of] a warrant issued based on a showing of probable cause.”)

⁷⁷18 U.S.C. § 2703(d).

⁷⁸50 U.S.C. § 1861(b)(2)(A).

demanding than that for a regular subpoena. On the other hand, these statutes do not require a full probable cause warrant. One can argue about what precise standard should govern here. Our own sense is that some requirement of “specific and articulable facts” establishing something more than relevance—something like necessity or importance—to an investigation would be appropriate. The crucial point for present purposes, however, is that some intermediate class of data—less sensitive and less closely held than one's personal records yet more sensitive than other transactional records—should be understood to exist and should receive some kind of intermediate procedural and substantive protection.


Again, an order for production of this sort of material might come from a federal district court or it might come, in a national security investigation, from the FISA court. The showing required of the government to win production should be the same irrespective of the type of investigation. Importantly, material should never be presumed to be part of this category. Rather, transactional data that Congress does not specifically designate as covered by this statute should be presumptively treated as routine transactional material. It should require an affirmative political decision by Congress to assign this heightened protection.

The broad goal is an architecture in which the reasonable person who bothers to educate himself about the law can consider a piece of his mosaic data and immediately know—or at least have a pretty good idea—what the government must do in order to get it. Data that such a person would reasonably understand to be his would, like his other stuff in his private spaces, require a warrant to search. Material about him in the possession of others would be beyond his control and relatively easily obtained by investigators. But specifically-designated subsets of that information—his health records, maybe records of where he has gone culled from his cell phone or the planting of a tracking device, and maybe other types of records—would receive some heightened protection.

Conclusion

Regulating the diverse issues associated with the mosaic presents any number of extraordinarily difficult questions. In some ways, the question of government access is one of the simpler ones. We have, after all, models for government access to information of varying levels of sensitivity. We have, broadly speaking, a certain comfort level with the basic premises—government non-access except upon a showing sufficient to meet a known evidentiary predicate. Regulating this aspect of the mosaic is really a matter of making some basic choices regarding which information belongs in what sort of category and then conforming our laws more coherently to those choices.

By contrast, regulating other aspects of the mosaic involve conceptually very new ground—in particular, how to treat large aggregations of individually non-sensitive data voluntarily given to private third parties for lawful use that collectively paints a particularly revealing picture. In the long run, and the long



run will not be very long, this is a question we will have to confront. But it isn't an investigative question. The investigative question is more discrete: Can we imagine Kris' "simpler world" in which fewer statutes regulate more acquisition more comprehensively and less complicatedly? We think we can, and that doing so would add great clarity to what is now a muddle.

Authors

Benjamin Wittes is a senior fellow in Governance Studies at The Brookings Institution. He is the author of *Detention and Denial: The Case for Candor After Guantanamo*, forthcoming from the Brookings Institution Press. He is also the author of *Law and the Long War: The Future of Justice in the Age of Terror*, published in June 2008 by The Penguin Press, and the editor of the 2009 Brookings book, *Legislating the War on Terror: An Agenda for Reform*. He co-founded and co-writes the *Lawfare* blog (<http://www.lawfareblog.com/>), which is devoted to non-ideological discussion of the “Hard National Security Choices,” and is a member of the Hoover Institution Task Force on National Security and Law.

Wells C. Bennett is an Associate at Arnold & Porter LLP, where his practice focuses on issues implicating international law, as well as U.S. foreign relations and national security law. He is the co-author of “Better Rules for Terrorism Trials,” a chapter in *Legislating the War on Terror: An Agenda for Reform*. Before joining Arnold & Porter, he served as a law clerk for the Hon. Terrence W. Boyle, on the United States District Court for the Eastern District of North Carolina.

Rabea Benhalim is an attorney and graduate of the University of Texas at Austin School of Law and the University of Michigan Ford School of Public Policy. She is a coauthor of “The Emerging Law of Detention: The Guantánamo Habeas Cases as Lawmaking,” a Brookings monograph published in 2010.

Governance Studies

The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
www.brookings.edu/governance.aspx

Editor

Christine Jacobs

Production & Layout

John S Seo

E-mail your comments to
gscments@brookings.edu

This paper is distributed in the expectation that it may elicit useful comments and is subject to subsequent revision. The views expressed in this piece are those of the authors and should not be attributed to the staff, officers or trustees of the Brookings Institution.