Pre-publication draft. Cite to Alan Rubel, "Privacy, Transparency, and Accountability in the NSA's Bulk Metadata Program," in Adam Moore (ed.) *Privacy, Security, and Accountability*, Rowman & Littlefield International (2015)..

Privacy, Transparency, and Accountability in the NSA's Bulk Metadata Program

Alan Rubel
University of Wisconsin, Madison
arubel@wisc.edu

1. Introduction

Disputes at the intersection of national security, surveillance, civil liberties, and transparency are nothing new, but they have become a particularly prominent part of public discourse in the years since the attacks on the World Trade Center in September 2001. This is in part due to the dramatic nature of those attacks, in part based on significant legal developments after the attacks (classifying persons as "enemy combatants" outside the scope of traditional Geneva protections, legal memos by White House counsel providing rationale for torture, the USA Patriot Act), and in part because of the rapid development of communications and computing technologies that enable both greater connectivity among people and the greater ability to collect information about those connections.

One important way in which these questions intersect is in the controversy surrounding bulk collection of telephone metadata by the U.S. National Security Agency. The bulk metadata program (the "metadata program" or "program") involved court orders under section 215 of the USA Patriot Act requiring telecommunications companies to provide records about all calls the companies handled and the creation of database that the NSA could search. The program was revealed to the general public in June 2013 as part of the large document leak by Edward Snowden, a former contractor for the NSA.[1]

A fair amount has been written about section 215 and the bulk metadata program. Much of the commentary has focused on three discrete issues. First is whether the program is *legal*; that is, does the program comport with the language of the statute and is it consistent with Fourth Amendment protections against unreasonable searches and seizures? Second is whether the program infringes privacy rights; that is, does bulk metadata collection diminish individual privacy in a way that rises to the level that it infringes persons' rights to privacy? Third is whether the secrecy of the program is inconsistent with democratic accountability. After all, people in the general public only became aware of the metadata program via the Snowden leaks; absent those leaks, there would have not likely been the sort of political backlash and investigation necessary to provide some kind of accountability.

In this paper I argue that we need to look at these not as discrete questions, but as intersecting ones. The metadata program is not simply a legal problem (though it is one); it is not simply a privacy problem (though it is one); and it is not simply a secrecy problem (though it is one). Instead, the importance of the metadata program is the way in which these problems intersect and reinforce one another. Specifically, I will argue that the intersection of the questions undermines the value of rights, and that this is a deeper and more far-reaching moral problem than each of the component questions.

The paper is organized as follows. In part 2 I explain the section and its legal basis; I argue that the section is plausibly legal, but that it is based on a very permissive interpretation of the law. In part 3 I

[1] Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily"; Greenwald and Ball, "The Top Secret Rules That Allow NSA to Use US Data without a Warrant."

argue that although the program affects privacy rights, it is at least plausible that those rights are not unjustifiably infringed. In section 4 I address the question of the program's transparency, and argue that it is indeed a problem (though largely because of the legal and privacy questions). Finally, in section 5 I argue that the deeper and more far-reaching worry is that because of the mix of legal, privacy, and transparency problems the metadata program undermines the *value of whatever privacy rights we have*.

2. The Program and Its Legal Basis

2.1 Section 215 Record Collection

Section 215 of the USA Patriot Act (the "business records" provision),[2] allows the FBI to obtain a court order requiring other entities to produce "any tangible thing"—including any records—in order to protect against international terrorism. Specifically, it provides that

> the Director of the Federal Bureau of Investigation or a designee of the Director…may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items for an investigation to obtain foreign intelligence information…to protect against international terrorism or clandestine intelligence activities….

There are several limitations to the FBI's ability to collect information under §215. Most importantly, there must be some grounds for believing that the items and records sought are "relevant to an authorized investigation."[3] The FBI may not conduct an investigation based "solely" on activities protected by the First Amendment of the U.S. Constitution, and the FBI must follow "minimization procedures" that limit the extent to which tangible things can be retained, disseminated, and used.[4]

Tangible things.

The design of the bulk telephone metadata program tracks section 215's basic features. To begin, the program collects records about telephone calls, and not the contents of calls. When one makes or receives a telephone call, one's phone company automatically creates a record of certain call details, including (for example) the number dialed/received, the call's time, date, and duration, trunk identifier, and calling card numbers used. Because the information is merely "about" the call, and not the contents of the call itself, it is called "metadata"—a term long familiar in information studies fields, but becoming popularized in the wake of the Snowden leaks. The records that phone companies keep of call metadata are "tangible things" and hence eligible for production under section 215.

Based on section 215, the Foreign Intelligence Surveillance Court (FISC or "FISA Court") approved the National Security Agency's (NSA) request for an order to obtain "all call detail records"

[2] 50 U.S.C. §1861.
[3] 50 U.S.C. §1861(b)(2)(A). An investigation is "authorized" in turn, if it is approved by the U.S. Attorney General under an appropriate executive order and *not* conducted on U.S. persons based on solely on First Amendment protected activities. 50 U.S.C. §1861(a)(2).
[4] 50 U.S.C. §1861(a)(1)-(2), (b)(2)(B).

from certain phone companies in the U.S.[5] In practice, this means that phone companies subject to the order must provide the NSA with all records pertaining to phone calls to and from its customers, and most of the data provided comes from calls between persons in the U.S.[6] Although phone companies collect information about the locations of mobile phones when calls are made (based on the locations of cellular towers used sending and receiving signals), phone companies do not currently provide that information to the NSA.[7] However, the NSA has collected such information in the past in order to test whether it would be feasible to incorporate into the bulk metadata program, and some location information may be inferred from other metadata collected (e.g., area codes for landline phones and trunk identifiers). The order requires phone companies to produce the relevant records on a daily basis, and the NSA must request the FISA court to renew the order every 90 days.

Relevant to.

Even though metadata records are clearly "tangible things" under section 215, that is not a sufficient legal basis to receive a court order. Rather, the request for an order must be based on "reasonable grounds to believe that the [records] are *relevant to*" a foreign intelligence or terrorism investigation.[8] The FISA Court has determined that the relevance standard is low hurdle. Specifically, it has determined that relevance depends on whether information sought is "necessary for NSA to employ tools that are likely to generate useful investigative leads to help identify and track terrorist operatives."[9] The court accepts the premises that bulk data collection is necessary to identify the much smaller subset of terrorist communications and that making connections among communications is likely to generate useful investigative leads that help identify and track terrorist operatives. Hence, the court concludes that the bulk metadata program meets the section 215 relevance requirement.[10] That is, in order to ensure that the metadata for terrorist communications is included in its data, the NSA must collect all the metadata. Moreover, because the value of metadata may be apparent only after connections have been established, the FISA Court has determined that the information must be collected on an ongoing basis to ensure that historic information is not lost.[11]

Minimization procedures.

Although the relevance standard under section 215 is broad, the retention and use of the bulk metadata is limited by minimization requirements, which are a required component of the FBI's application for a court order under section 215.[12] The government is prohibited from accessing the data

[5] Oversight committee, page 22. Primary order "in re application, FISA court oct 11, 2013, page 3. There is some dispute about just which phone companies are subject to these ongoing orders.
[6] Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, 22.
[7] Ibid.
[8] 50 U.S.C. §1861(b)(2)(A) (emphasis added).
[9] "Primary Order," p. 20, quoting prior, redacted order.
[10] "Primary Order."
[11] Ibid.
[12] 50 U.S.C. §1861(b)(2)(B).

for any other intelligence or investigative purpose.[13] Hence, the data may not be used for general law enforcement purposes. Only certain trained, authorized persons have access to the data; access is afforded only via a query process, which in turn must be based on reasonable, articulable suspicion.[14] Information is kept for years. The government must notify the FISA court immediately of any cases of non-compliance.

The bulk metadata is consolidated, and analysts may only use the consolidated data by making queries. The records are searched based on a telephone number, or some other selection term, which is used as a seed. In order to perform such a search, one of a small number of NSA officials must determine that there is "reasonable, articulable suspicion that the selection term is associated with terrorism."[15] It is unclear what it means for a phone number to be "associated with terrorism."

The result of these minimization procedures is that "[t]he vast majority of the records the NSA collects are never seen by any person."[16] Oversight, p. 26, citing Shea declaration paragraph 23. "Only the tiny fraction of the telephony metadata records that are responsive to queries authorized under the RAS standard are extracted, reviewed, or disseminated by NSA intelligence analysts, and only under carefully controlled circumstances."[17]

So, because the metadata is based on business records, which are "tangible things" under section 215, because they are in some sense relevant to ongoing investigations, and because the NSA has minimization procedures in place, the program appears at least facially consistent with the FISA statute.

2.2 Constitutional Basis

Regardless of whether the bulk metadata program is consistent with the FBI's and NSA's statutory authority under section 215, there is a question as to whether it is consistent with the government constitutional limits under the Fourth Amendment of the U.S. Constitution. The Fourth Amendment provides that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

[13] "Primary Order," 4.
[14] Ibid., 5.
[15] Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, 27. The reasonable, articulable suspicion standard is further specified in the primary order as follows: "based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion" that the number "is associated with" a terrorist organization identified in the FISA court's orders. Primary order at 7.
[16] Ibid., 26. (citing Shea declaration paragraph 23).
[17] Shea declaration paragraph 23.

In order to determine whether government information collection violates the Fourth Amendment requires determining, first, whether the government's actions constitutes a *search* (seizures are not at issue here). The amendment prohibits unreasonable searches and seizures; hence if information collection does not constitute a search, then (a fortiori) it cannot constitute an *unreasonable* search. There is a two-part test for determining whether an activity constitutes a search, which was established in *Katz v. United States*.[18] First, a person must have exhibited a subjective expectation of privacy, and second, that expectation must "be one that society is prepared to recognize as 'reasonable.'"[19] Often the two parts are shortened into the pithier question of whether a person "has a reasonable expectation of privacy."

Two cases are crucial in explaining the applicability of the *Katz* test to telephone metadata. The first is *U.S. v. Miller*.[20] In that case federal agents sought Miller's bank records via subpoena, having neither the probable cause nor the warrant required for searches under the Fourth Amendment. The Supreme Court determined, however, that business records held by third parties (here, banks) are not protected by the Fourth Amendment, as one does not have a reasonable expectation of privacy in those records. A person engaging in business with a bank voluntarily discloses financial information to the bank; she thereby "takes the risk…that the information will be conveyed by that person to the Government."[21]

The second case, *Smith v. Maryland*, is even more on point. Smith robbed a woman's home. After doing so, he began making threatening phone calls to her and drove past her house. The woman collected Smith's license plate information, and police were able learn his address and phone number. They then got the phone company to install, without a warrant, a device (a "pen register") that could record the numbers dialed from Smith's home. They used information gleaned from the device to obtain a warrant, searched Smith's home, and found evidence of the robbery. The Supreme Court determined that neither part of the *Katz* test was met. That is, people neither have an actual expectation of privacy in numbers dialed, nor would such an expectation be on that society would recognize as reasonable. The court reasoned that persons voluntarily reveal numbers dialed and received from their phones, and hence (as in *Miller*) they take the risk that such information will be revealed by the third parties to the government.[22]

A significant proportion of commentators on the program have concluded that it is consistent with statutory and constitutional law. One federal court has dismissed an action seeking injunction against the NSA's metadata collection, determining that the plaintiffs were unlikely to prevail on their claims that the program violates FISA and the Fourth Amendment.[23]

---

[18] 389 U.S. 347 (1967).
[19] Katz at 361.
[20] 425 U.S. 435 (1976).
[21] 425 U.S. at 443.
[22] 442 U.S. 735 (1979)
[23] ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013); see also Kris, "On the Bulk Collection of Tangible Things"; Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*.

2.3 Legal Criticisms

Despite the decision in the *Clapper* case, the academic support for the government's interpretation of section 215, and the Supreme Court's decisions rejecting the idea that gathering of third-party and transactional information constitutes a search under the Fourth Amendment, there is significant support for the view that the program is not consistent with the law.

One federal court has arrived at a different conclusion than the *Clapper* court. In *Klayman v. Obama*, No. 13-0851 (D.D.C. Dec. 16, 2013), the District Court for the District of Columbia granted (and subsequently stayed) a preliminary injunction against the NSA's collection of telephone metadata on Fourth Amendment grounds. Specifically, it determined that the bulk collection of metadata is sufficiently different from the pen register collection of numbers dialed by one phone that *Smith v. Maryland* isn't applicable. Rather the D.C. court found more relevant the recent case of *U.S. v. Jones*, in which the U.S. Supreme Court determined that placing a GPS device on a car and following it for several weeks constituted a search under the Fourth Amendment. There, a concurring opinion distinguished between long term monitoring and more isolated information gathering, allowing that constant following via GPS could constitute a search, even where discrete elements of that following would not. Following *Jones*, the D.C. court determined that bulk metadata collection could constitute a search even where discrete collection of metadata would not.

In addition to the constitutional claims, there are several criticisms based on section 215. The Privacy and Civil Liberties Oversight Board (PCLOB), an independent executive agency formed in response to recommendations made by the 9/11 Commission, issued a report on the bulk metadata program in January 2014. It found several flaws in the NSA's (and, hence, FISC's) interpretation of section 215, each of which casts some doubt on whether the program is legal.

First, the PCLOB questions the entity collecting the information. Section 215 authorizes the FBI to make business records requests. However, the bulk telephony metadata program is conducted by the NSA—an organization with a wholly separate mandate, statutory authorization, and leadership. Nothing in section 215 suggests that the FBI can transfer its authority or routinely share information gleaned pursuant to business records requests with other entities. Second, the PCLOB questions whether the metadata program collects information "relevant to" any ongoing investigation. While there are always some terrorism related investigations occurring, and hence the information is relevant to investigations in some sense, there is no particular investigation to which the program is relevant. Third, the board questions the practice of collecting records on a daily basis. Typically records requests are made retrospectively—there is an investigation, and pre-existing records are collected as part of that investigation. Here, though, there is a prospective order that requires collections of whatever records are produced each day. Finally, the PCLOB questions whether *Miller* and *Smith* are adequate to deal with contemporary capacities to gather information.

2.4 Legal Conclusions

In the end, it seems that the metadata program is plausibly legal, but it pushes against even very expansive interpretations of section 215 and Fourth Amendment law. The agency conducting the

program (the NSA) is different than the agency authorized to make the requests under section 215 (the FBI). The interpretation of "relevance" under section 215 is so broad that it would render almost any vast collection of persons' information legal and the "relevance" of most information gathered depends on the information collected being exhaustive. There is no connection to any specific investigation, and new records are produced daily rather than in response to new requests. Moreover, although collection of metadata is not a Fourth Amendment search under *Smith v. Maryland*, that case is four decades old, and the technological change may have rendered it obsolete, especially in consideration of the "mosaic theory" advanced under a concurrence in *U.S. v. Jones*.

3. Privacy Rights

In the previous section I argued that the primary concern with the bulk metadata program cannot be its legality. The program rests on a permissive, aggressive, and envelope-pushing legal interpretations, but is nonetheless at least plausibly legal. The program is also problematic on the grounds of privacy, regardless of the program's legality. However, criticizing the program on straightforward privacy grounds also has some important limitations.

People have at least some moral rights to privacy. By this I just mean that there are some cases in which individuals have valid claims that others not surveill, collect information about, monitor, or distribute information about them, and those claims are the individuals' moral due.[24] It is this right that allows one to justifiably assert that, for example, one has been wronged by others listening in on one's phone calls without permission, or that one has been wronged by an insurance company publishing one's health information for the world to see. I won't spend much time arguing for this right, for a couple of reasons. First, there is a substantial literature on privacy and privacy rights already. Accounts of the basis for privacy rights include those focused the importance of privacy in human well-being and flourishing, privacy being the object of persons' autonomous choices, privacy being at times a *condition* of autonomous choice, privacy as an important condition for liberal democracy, and privacy as a condition for many and varied social relationships.[25] More important, though, is that absent valid claims to privacy (which is to say, privacy rights), arguments about whether bulk metadata collection (or any other surveillance program) is justified can't get off the ground. This is not to say that all things considered the metadata program is unjustified. Rather, it is to say that *if* the metadata program is justified, it either does not infringe whatever privacy rights we have, or that if it does infringe privacy rights, other considerations are sufficient to override privacy rights.

That the metadata program affects privacy should be uncontroversial. The section 215 orders required that telecommunications providers provide the NSA with metadata from all cell phone calls using their networks. As a result, information about individual cell phone users and their calls end up in a database that can be easily queried by federal agents. And even though that metadata is collected in the course of telecommunications business, the orders expanded the range of persons able to access

[24] Feinberg, "The Nature and Value of Rights."
[25] Gavison, "Privacy and the Limits of Law"; Moore, *Privacy Rights*; Allen, *Unpopular Privacy*; DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*; Benn, "Privacy, Freedom, and Respect for Persons"; Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser"; Reiman, "Privacy, Intimacy, and Personhood."

and make use of that information. Hence, individuals' privacy regarding their cell phone communications decreased with respect to the federal government. Given the minimal account of privacy rights I suggest above, it follows fairly easily that the program infringes privacy rights. We have some moral claim that government actors not collect information about the people with whom we communicate, and the metadata program does just this. Now, because that is a fairly austere account of privacy rights, it remains an open question whether the infringement here is substantial, and whether benefits of the program suffice to override those rights. There are some reasons to think the infringement is not substantial and that the benefits may outweigh it.[26]

First, the information collected in the context of the metadata program is limited. Specifically, the section 215 court orders request numbers dialed, numbers of calls received, call durations, trunk identifier information, and similar transactional information. The NSA does not collect information about the content of phone calls, and it does not collect phone locations (at least not in this particular program). Certainly who one communicates with and for how long is information in which one may have a privacy right. But it is arguably less intrusive than lots of other types of information: GPS location information, eavesdropping on call content, computer searches. Of course, the fact that there are more intrusive means of surveillance does not entail that lesser intrusions are permissible.

Second, the information collected as part of the program is already systematically collected by telecommunications companies. The metadata at the heart of the program (numbers called, call durations, and so forth) is information that telecommunications companies must collect simply in order to provide services. Hence, independently of whether the metadata program existed, any user of those services would not have privacy regarding her telephone metadata with respect to her telecommunications provider. The metadata program simply extends the group of entities having access to that information to include the NSA. While this decreases people's privacy, the moral weight of the decrease would seem to be less than if the information were not already collected for reasons unrelated to the metadata program. Third, the program includes minimization procedures. Specifically, the database created from the records could be searched only by querying the database based on a "seed" number, for which agents had reasonable suspicion of a connection to a foreign intelligence. It was not subject to browsing, or to querying based on other numbers.

The last consideration is that, even if we suppose that the program affects privacy rights, do we have good reason to think that the program is effective enough to justify any infringement? Perhaps so. There is significant controversy as to whether the program leads to gains in security.[27] The PCLOB has

[26] It is worth pausing to note something about the nature of the argument here. It is possible that the metadata program is a very momentous violation of privacy right, and that that violation is great enough that even very large benefits to most people couldn't justify overriding the rights. Such an argument would not conflict with my arguments here. My strategy is instead to point out why there is something more going on with respect to rights (viz., that the intersection of problems in this case undermines the value of rights to right-holders). By making that case even on the assumption that privacy rights are infringed only slightly, or that they are infringed justifiably, I hope to show that the program is, all things considered, unjustifiable. If I'm right, then the program will also be unjustified (*a fortiori*) if privacy rights infringements are graver, and where there is insufficient grounds to override them.

[27] Bergen et al, "Do NSA's Bulk Surveillance Programs Stop Terrorists?" New America Foundation, January 2014.

concluded that there is at least *some* benefit to the program, if limited.[28] And in a separate statement, one member of the PCLOB stressed that the *future potential* benefits of the program provide justification for its existence.[29] Of course such an argument has important gaps. It rests on a substantial and speculative empirical claim. Moreover, even if there is some benefit, it cannot tell us whether that benefit is great enough to subsume the privacy rights at issue. Nonetheless, whatever the benefits of the program are, they mitigate the degree to which privacy rights are themselves dispositive.

So, there is no question that our privacy diminishes based on the metadata program, and it plausibly infringes privacy rights. But there are important limitations on the degree to which it infringes privacy rights: the type of information collected, the fact that telecommunications companies collect the information in any case, the limitations on use, and the fact that many of us will feel no ill effects. And while we should be skeptical of claims about the efficacy of the program, the possibility of its efficacy may serve to justify the rights infringement. Here I want to be clear that I am not arguing that the program is, all things considered, a justifiable infringement of privacy. Rather, I am arguing that the discrete privacy concerns cannot really explain the depth of worry about the program.

4. Transparency

A third question surrounding the metadata program centers on its secrecy. Requests for section 215 court orders are issued to the Foreign Intelligence Surveillance Court (the FISC, or FISA court). That court meets in secret, and hence the orders are themselves secret. Moreover, the existence of the program was unknown until (and would likely never have been revealed but for) the Edward Snowden revelations in 2013.

The mere fact that some court orders are secret is a criticism of the existence of the FISC in the first instance, rather than a criticism of the metadata program overall. But the existence of a secret, widespread, and longstanding surveillance program is more problematic. This is a case in which the phone data of every person in the U.S. was potentially collected and stored, and yet no one in the general public was aware of the program. There is no question that some facets of government require at least a degree of secrecy in order to be effective, and the precise contours of a surveillance program are plausibly such a case.

However, as Dennis Thompson has argued, lest we abandon the possibility of democratic accountability for security programs altogether, there must at least be a kind of "second order" transparency. That is, we must have an idea about the kind of policy or practice that is largely carried out in secret.[30] It would appear though that there is no second-order transparency in the case of the metadata program. That is because the legal interpretation on which the program is based pushed so forcefully against the plausible bounds of statutory law. Not only was the program itself secret, but the legal interpretation of section 215 on which it is based was secret. More importantly still, that interpretation was one that no person could reasonably have anticipated to have been operating within the FBI and NSA. As outlined in section 2, although the program is plausibly legal, it is so only when we read the statute with the specifics of the metadata program in mind. The government's interpretation of

[28] Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, 144–155.
[29] Ibid., 212. (Separate statement by member Rachel Brand.)
[30] Thompson, "Democratic Secrecy."

'relevance' is envelope-pushing, and the metadata collected is relevant to 'an authorized investigation' only insofar as there are continuously *some* authorized investigations occurring. No one interpreting the statute without already knowing of the metadata program could reasonably anticipate that section 215 could support such widespread information collection. Hence, there is a failure of even second-order transparency.

5. Undermining the value of rights

In the previous sections, I have argued that (1) the metadata program is plausibly legal, though based on an envelope-pushing statutory interpretation, (2) the metadata program infringes privacy rights, but that those infringements are limited and possibly justified by benefits, and (3) that there are important transparency problems both in the secrecy of the program and the obscurity of the legal interpretation on which it is based. But the deeper problem with the program is the way the legal issue, the privacy issue, and transparency issue intersect. Specifically, that intersection undermines the value of rights to right-holders.

Elsewhere, I have argued that there is an important distinction to be made between rights themselves and the value of rights to right-holders, and that under certain conditions there is an obligation to ensure the full value of rights to right-holders.[31] That obligation is independent of whether the original right is itself infringed, and it is independent of whether the right itself is justifiably infringed.

To illustrate the distinction I have in mind, consider the right to access government records. In the U.S., the Freedom of Information Act (FOIA) provides people the right to access documents created by the federal government; all fifty U.S. states have similar laws that pertain to state and local government information. These are legal rights, but they are justified by a moral right to have important information about a government acting on one's behalf, a right to be governed only under conditions to which reasonable persons could consent, and the instrumental values of making easy use of information and helping ensure reasonably good governance. The right to access government records includes the ability to receive information upon request, the assurance that the government actually retain important records, and that any costs to access be reasonable. Now compare the governments of two similar states: Cheese State and Beer State. The government of Cheese State keeps its records in electronic format, and can provide (for example) property records, budgets, meeting minutes, reports, and so forth via the Internet in machine-readable form. This allows people making records requests to get information quickly and to easily search, extract, and compile information in the records. In contrast, the government of Beer State keeps its records on paper only. Responding to information requests in Beer State requires that files be copied or scanned (which takes longer), and it is much more difficult to search, extract, and compile data from Beer State records. In both Cheese State and Beer State, people have fully intact rights to access government records. However, the *value* of the right to people in Cheese State is greater because they are better able to make use of the right.[32]

---

[31] Rubel, "Privacy and the USA Patriot Act: Rights, the Value of Rights, and Autonomy"; Rubel, "Profiling, Information Collection and the Value of Rights Argument."

[32] Other examples include the right to vote and the right to expression. One might have a fully intact right to vote (access to polls, vote counts the same as others, and one's choice holds sway if it is shared by required proportion of voters), but have that vote be of little value because one does not have sufficient information to distinguish

What matters here is the *objective* value of the right, or the ability of the right-holder to make use of the right or to benefit from the right should the right-holder need to. This contrasts with the subjective value of a right, or the degree to which right-holders subjectively value a right. So, in the open records case, Attie might not care much about the form in which her state will provide access to records as a general matter; indeed, she might not even be aware of her access rights. Suppose, though, that she wishes to invest in property, and would like to search the property records of dozens of parcels in a short period of time. It would be much easier for her to conduct that search if the records are kept in electronic form. Hence, the value of the right is greater to her objectively, even if she doesn't realize it.

Now, under some circumstances states have an obligation to ensure the full value of rights to right-holders, though not always. Consider the right to vote. That right is more valuable to an individual right-holder where she can sell her votes to the highest bidder.[33] But surely the state has no obligation to permit such sales, even though the objective value of the right to the right-holder is diminished where selling votes is prohibited. Compare, though, the case in which a person has a right to vote, but lacks sufficient information about candidates or issues to make a reasonable decision in an election. There, it is at least plausible that the state has failed in a responsibility to ensure that the right to vote is valuable to right-holders. The difference in the two cases is that in the vote-selling case the value of the right to the right-holder conflicts with the justification for the existence of the right in the first place, whereas in the low-information case the value of the right *aligns* with underlying justification. The right to vote is justified in order to ensure that government reflects (at least to some degree) the will of its people, as a means for people to exercise political self-direction, and to encourage democratic accountability. Each of those depends on (among other things) voters having adequate information; each is thwarted to the extent that people can sell their votes.[34]

There are other criteria to determine whether states have an obligation to secure the full value of rights. One is that state action precipitates a right's diminished value. Consider again the open records example. A state's failure to digitize records is plausibly a failure of its duty to secure the value of the right to access information. In contrast, if Attie does not have the financial resources to invest in property, her right of access to property records is less valuable to her (objectively), but it would not seem that the state has an obligation to secure the value in that case. Another criteria is that states only have obligations to secure the full value of rights where they can actually do so, for one cannot have an obligation to do something that one is unable to do.

Privacy

How, then, does the value of rights bear upon the metadata program? Consider first the right to privacy. As noted in section 3, there are a number of different justifications for privacy rights. Instrumental accounts base privacy's value on what it does: providing space for individuals to function and flourish, establishing a condition in which many and varied social relationships can exist and thrive, and preventing others from treating individuals unfairly on the basis of personal information. On other views, privacy is important based on persons' autonomy, or the ability to determine for oneself what one values, and to act according to those values as one sees fit. Privacy can be the *object* of autonomous

choices. Similarly, one might have a fully intact right to free expression, but that right might be of less value insofar as one lacks financial resources to broadcast or distribute one's expression. See Rubel (2007) and Rubel (2013).

[33] This example come from Rubel, "Profiling, Information Collection and the Value of Rights Argument."

[34] Ibid.

action, as when one determines that it is important to act and make decisions without the scrutiny of others. And as Stanley Benn has argued, the nature of and meaning of persons' actions may change depending on whether others observe those actions; an action done for its own sake is distinguishable, on this view, from an action done partly for the sake of an observer.[35] Privacy may also be a *condition* of autonomous choice; where one is closely surveilled, the degree to which their views, projects, and actions are the result of their own deliberation rather than others diminishes.[36]

In part 3 I claimed that the metadata program infringes privacy rights (though perhaps justifiably). More problematic is the way that the program undermines the value of privacy rights to right-holders. It does this in several ways. First, the fact that the program was secret made it impossible for people *tell* whether their privacy was diminished by the federal government. Of course, whether one can tell that her rights have been infringed is a different matter from whether those right have actually been infringed, and hence the secrecy of the program cannot be an infringement of the privacy right itself. Why, though, does the inability to tell whether one's privacy has been infringed diminish the value of the privacy right? Among the justifications for rights to privacy is that they are instrumentally important (for the salubrious effects having distance from scrutiny, for opportunities to flourish, for political processes, for varied relationships). Strictly speaking, these depend on *beliefs* about privacy. The secrecy of the program prevents people from knowing the status of their privacy; preventing people from being able to interpret their circumstances, in particular their circumstances with respect to an important right is an affront to their autonomy.[37] And that affront to autonomy is independent of whether people would change their actions based on knowledge of surveillance, and independent of whether the surveillance is (considered by itself) a justified infringement of privacy rights.

The secrecy of the metadata program itself is only part of the way it diminishes the value of rights. At least as important is the aggressive legal interpretation on which the program is based, described in section 2, and which I explained in section 4 is an interpretation that no one could reasonably anticipate without some prior knowledge of the program. The inability to interpret statutes and constitutional provisions that protect rights means that a person cannot reasonably anticipate the *types* of rights infringements that one is likely to endure. So, while the secrecy of the program conflicts with autonomy interests by precluding one from understanding just how she is being treated ("am I being surveilled?"), the aggressiveness and secrecy of the legal interpretations conflicts with an autonomy interest in anticipating the *rules governing* how one is treated ("could I be legally surveilled?").

A third, and related, way in which the program undermines the value of privacy rights is that it forestalls persons' opportunities to *assert* or *claim* their moral due. While rights protect interests (in well-being, in autonomy, in political processes), as Joel Feinberg has argued the importance of rights includes the fact that right-holders can assert them.[38] Persons' interests may be harmed in myriad ways. Sometimes it is based on broad phenomena to which a person may object, but with respect to which she has no right. So, a policy decision to (e.g.) build a metro line in location A rather than location B

[35] Benn, "Privacy, Freedom, and Respect for Persons," 228–29.
[36] Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser."
[37] Rubel, "Privacy and the USA Patriot Act: Rights, the Value of Rights, and Autonomy"; Hill, "Autonomy and Benevolent Lies."
[38] Feinberg, "The Nature and Value of Rights."

might harm Lucille in that she stood to benefit from having it in location B, and perhaps even invested in property on the hope that the line would be in location B. But that would not infringe a right, and she cannot assert some individual claim to have the line where she wishes. In contrast, rights warrant individuals to make claims. Privacy rights allow one to say that "*I* have a claim that others not collect my information." But where rights infringements are secret, as in the case of the metadata program, it is impossible to assert such a claim.

So, the metadata program does more than infringe privacy rights. The lack of transparency surrounding the program (including both the existence of such a program and the obscurity of the interpretation of the legal interpretation underwriting) make whatever privacy rights we actually have less valuable. The value that is diminished is in each case part of the value that justifies the right in the first place (autonomy, the ability to make use of rights, the ability to assert or claim rights). And because those actions are the result of state action, and because it is within the state's power to disclose the existence of surveillance programs and (more important) issue more reasonable legal interpretation, this is a failure of a duty to secure the value of privacy and other rights.

Transparency

Next, consider transparency, and the right to information about government action. A right to information about the workings of the state is grounded partly in instrumental values, including the role of transparency in preventing corruption and abuse of power. And it is grounded partly in the principle that government is legitimate only with consent of the governed (an autonomy-view). Exactly what consent demands in this case is controversial. Perhaps the most prominent account in recent decades is Rawls's view that legitimate exercise of government power demands that it be consistent with constitutional principles that "all citizens as free and equal may reasonably be expected to endorse in the light of principles and ideals acceptable to their common human reason."[39]

In some ways the secrecy of the metadata program (both the program itself and the legal interpretations on which it is based) would appear only to conflict with rights to information about government. After all, how could the mere lack of transparency *also* diminish the value of rights to government information? What is important here is that the lack of transparency concerns an important moral and legal right. This is not an issue of how a narrow administrative rule or specialized statute is interpreted. Rather, it is a right that has substantial statutory and constitutional protections. While secret actions and obscure interpretations pose problems of transparency and accountability in any case, where they affect basic rights and liberties the problem runs deeper. The weightier the value of the right subject to secret action and secret legal interpretation, the greater the loss of the value of that right due to the secrecy.

Further, such aggressive and secretive legal interpretation infects other rights. Specifically, it allows persons to infer that the government is likely to pursue other aggressive interpretations of the law of which we will be unaware. Part of the value of rights is that they allow individuals to act with some confidence in their belief that the interests grounding the rights are in fact protected. And yet here is a case in which an arm of the executive has received judicial approval in secret for legal interpretations that circumscribe a moral right by narrowing the legal protections for that right. There is, hence, much less reason to think that the government will reasonably, and openly, interpret other

[39] Rawls, *Political Liberalism*, 137.

statutes and constitutional provisions in a way that tends to protect rather than undermine the interests protected. In light of the interpretations underwriting the program it is more plausible to believe, and more reasonable to act as if, the government will also aggressively and secretly interpret protections for expression and assembly, religious practice, equal protection, and due process.[40] To the extent that the value of rights includes being able to act on the assumption that they are secured, the metadata program (and the legal interpretations on which it is based) diminish the value of other rights, too. And that is true regardless of whether those other rights are indeed at risk.

This diminishment of the value of rights conflicts with a key value that justifies transparency in the first place. It is difficult to see that people could endorse a system in which the government interprets laws protecting persons' rights in ways that are at once secret and impossible to anticipate. It would seem, in other words, that persons could not reasonably be expected to endorse principles that preclude their understanding of how their de jure rights are to be treated.

The Intersection

At this point it is worth stepping back and considering the intersection of legal interpretation, privacy rights, and transparency. The mere fact that the government has promulgated an aggressive, envelope-pushing interpretation of the law matters. But that alone is not deeply problematic insofar as lawyers and governments often advance such arguments. The nature and extent of information collection in the metadata program is important, too. However, the program's effect on privacy has important limits based on the nature of the information collected, the fact that the information is collected by different parties in any case, and the potential benefits of the program. And transparency itself is important, but some government secrecy is justifiable.

Notice, though, the picture that emerges when we consider the intersection between these issues. First, the secrecy in this case is not just any secrecy; rather, it is secrecy *about* an aggressive, envelope-pushing legal interpretation. And as a result, people were denied the second-order transparency that is crucial to ensure that some secrecy is compatible with democratic governance.

Second, because the privacy loss was secret (both in fact and in legal interpretation), persons were denied the full value of their privacy rights. In other words, the metadata program is not merely about privacy loss, but the inability to actually make use of privacy rights because people did not know their privacy was diminished. And hence, their autonomy was circumvented in that they were unable to fully interpret important facts about their treatment, and people were unable to actually assert their rights. Third, because the secrecy and aggressive legal interpretations were about an important right, it makes less reasonable persons' beliers in the security of other basic rights, and hence undermines the value of *those* rights to the right-holders. In other words, the importance of metadata program is the

[40] Indeed, there are other cases that fit this pattern. Consider, for example, the particularly aggressive and secret interpretations of laws prohibiting torture. See, for example, Memorandum from Office of the Assistant Att'y Gen. to Alberto R. Gonzales, Counsel to the President (Aug. 1, 2002) (the "Bybee memo"), available at https://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB127/02.08.01.pdf; Memorandum from John Yoo, Deputy Assistant Att'y Gen., & Robert J. Delahunty, Special Counsel, to William J. Haynes II, Gen. Counsel, Dep't of Def., available at http://nsarchive.gwu.edu/NSAEBB/NSAEBB127/02.01.09.pdf Waldron, "Torture and Positive Law"; The New York Times, "A Guide to the Memos on Torture."

way in which problems legal interpretation, privacy, and transparency work together to render rights less valuable.

6. Conclusion

My goal in this paper is to look at several objections to the section 215 metadata program, each of which is important but limited, and to explain why we need to consider the links between those objections rather than viewing them in isolation. So, while the program presents a legal problem insofar as it is based on aggressive, envelope-pushing legal interpretations, those interpretations are a deeper worry because they are (1) secret, and (2) about an important right. And while the program presents a privacy problem by collecting lots of information about US persons, that privacy issue is deeper problem because it was (1) secret, and (2) based on legal interpretations that were also secret. Finally, while the secrecy of the program presents a problem of government transparency, that lack of transparency presents a deeper problem because it (1) concerned a legal interpretation that no one could reasonably have anticipated (rather than mere secrecy about the program specifics), and (2) concerned an important right. In the end, one might still argue that the program is justified, all things considered. But such an argument won't be sound unless it addresses the intersection of legal interpretation, privacy, and secrecy, and how that intersection undermines the value of rights.

Allen, Anita L. *Unpopular Privacy: What Must We Hide?*. Studies in Feminist Philosophy. Oxford ; New York: Oxford University Press, 2011.

Benn, Stanley I. "Privacy, Freedom, and Respect for Persons." In *Philosophical Dimensions of Privacy: An Anthology*, edited by Ferdinand David Schoeman. Cambridge [Cambridgeshire] ; New York: Cambridge University Press, 1984.

Bloustein, Edward. "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser." *New York University Law Review* 39 (1964): 962–1007.

DeCew, Judith Wagner. *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithaca, N.Y.: Cornell University Press, 1997.

Feinberg, Joel. "The Nature and Value of Rights." In *Rights, Justice, and the Bounds of Liberty: Essays in Social Philosophy*, 143–58. Princeton, NJ: Princeton University Press, 1980.

Gavison, Ruth. "Privacy and the Limits of Law." *The Yale Law Journal* 89, no. 3 (January 1, 1980): 421–71. doi:10.2307/795891.

Greenwald, Glenn. "NSA Collecting Phone Records of Millions of Verizon Customers Daily." *The Guardian*. Accessed March 23, 2015. http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

Greenwald, Glenn, and James Ball. "The Top Secret Rules That Allow NSA to Use US Data without a Warrant." *The Guardian*. Accessed March 23, 2015. http://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant.

Hill, Thomas Jr. "Autonomy and Benevolent Lies." *Journal of Value Inquiry* 18 (1984): 251–97.

"In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, No. BR 13-158 FISA Ct. (Oct. 11, 2013)," n.d.

Kris, David S. "On the Bulk Collection of Tangible Things." *Journal of National Security Law & Policy* 7 (2014): 209–95.

Moore, Adam D. *Privacy Rights: Moral and Legal Foundations*. University Park, Pa: Pennsylvania State University Press, 2010.

Privacy and Civil Liberties Oversight Board. *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, January 23, 2014.

Rawls, John. *Political Liberalism*. The John Dewey Essays in Philosophy, no. 4. New York: Columbia University Press, 1996.

Reiman, Jeffrey H. "Privacy, Intimacy, and Personhood." *Philosophy and Public Affairs* 6, no. 1 (Autumn 1976): 26–44.

Rubel, Alan. "Privacy and the USA Patriot Act: Rights, the Value of Rights, and Autonomy." *Law and Philosophy* 26, no. 2 (2007): 119–59.

———. "Profiling, Information Collection and the Value of Rights Argument." *Criminal Justice Ethics* 32, no. 3 (December 1, 2013): 210–30. doi:10.1080/0731129X.2013.860729.

The New York Times. "A Guide to the Memos on Torture." *The New York Times*, June 25, 2004, sec. International. http://www.nytimes.com/ref/international/24MEMO-GUIDE.html.

Thompson, Dennis F. "Democratic Secrecy." *Political Science Quarterly* 114, no. 2 (July 1, 1999): 181–93. doi:10.2307/2657736.

Waldron, Jeremy. "Torture and Positive Law: Jurisprudence for the White House." *Columbia Law Review* 105 (2005): 1681.