LEGAL ARCHETYPES AND METADATA COLLECTION

ALAN RUBEL*

INTRODUCTION

In discussions of state surveillance, the values of privacy and security are often set against one another, and people often ask whether privacy is *more important* than national security.[1] I will argue that in one sense privacy is more important than national security. Just what *more important* means is its own question, though, so I will be more precise. I will argue that national security rationales cannot by themselves justify some kinds of encroachments on individual privacy (including some kinds that the United States has conducted). Specifically, I turn my attention to a recent, well publicized, and recently amended statute (Section 215 of the USA Patriot Act[2]), a surveillance program based on

* Alan Rubel is an associate professor at the Information School and in the Legal Studies Program at the University of Wisconsin-Madison. This paper is based on a presentation at the Wisconsin International Law Journal's 2016 Symposium. I wish to thank the participants in that meeting for their insightful commentary and discussion.

1 Among the key questions that the journal editors ask in motivating their 2016 symposium is whether privacy is more important than national security. They explained that "[d]ata retention, surveillance, and similar laws are continuously challenged on the ground that they infringe upon individuals' privacy. In some countries, such as the United States, the needs of law enforcement often outweigh individual privacy, allowing for agencies like the NSA to surveil U.S. citizens." WIS. INT'L L.J. ANN. SYMP., 2016 (Apr. 8, 2016), https://law.wisc.edu/wilj/.

2 USA PATRIOT Act, Pub. L. No. 107-56, § 215, 115 Stat. 272, 286–87 (2001) (codified as amended at 50 U.S.C. § 1861).

that statute (the National Security Agency's bulk metadata collection program), and a recent change to that statute that addresses some of the public controversy surrounding the surveillance program (the USA Freedom Act).[3] That process (a statute enabling surveillance, a program abiding by that statute, a public controversy, and a change in the law) looks like a paradigm case of law working as it should; but I am not so sure. While the program was plausibly legal, I will argue that it was morally and legally unjustifiable. Specifically, I will argue that the interpretations of Section 215 that supported the program violate what Jeremy Waldron calls "legal archetypes,"[4] and that changes to the law illustrate one of the central features of legal archetypes and violation of legal archetypes.

The paper proceeds as follows: I begin in Part I by setting out what I call the "basic argument" in favor of surveillance programs. This is strictly a moral argument about the conditions under which surveillance in the service of national security can be justified. In Part II, I turn to Section 215 and the bulk metadata surveillance program based on that section. I will argue that the program was plausibly legal, though based on an aggressive, envelope-pushing interpretation of the statute. I conclude Part II by describing the USA Freedom Act, which amends Section 215 in important ways. In Part III, I change tack. Rather than offering an argument for the conditions under which surveillance is justified (as in Part I), I use the discussion of the legal interpretations underlying the metadata program to describe a key ambiguity in the basic argument, and to explain a distinct concern in the program. Specifically that it undermines a legal archetype. Moreover, while the USA Freedom Act does not violate legal archetypes, and hence meets a condition for justifiability, it helps illustrate why the bulk metadata program did violate archetypes.

I. THE BASIC ARGUMENT

There is no shortage of political, academic, and popular commentary on the Section 215 bulk metadata program. Some focus on legal questions. For example, does the program violate the Foreign

---

[3] USA FREEDOM Act, Pub. L. No. 114–23, § 101, 129 Stat. 268, 269–71 (2015) (codified as amended at 50 U.S.C. § 1861).

[4] *See* Jeremy Waldron, *Torture and Positive Law: Jurisprudence for the White House*, 105 COLUM. L. REV. 1681, 1718 (2005).

Intelligence Surveillance Act (FISA)?[5] Is it constitutional?[6] A substantial amount of the commentaries consider whether the program is effective (has it thwarted any attacks?).[7] Still others focus on what sort of inferences government actors could make using telephone metadata, and a number of pieces consider whether we have reason to be concerned about government actors collecting the data and making those inferences.[8] Each of these discussions is important. To set the stage for this paper I wish to step back and consider what it would take to justify a program like bulk telephone metadata collection.

The first thing to do is to get straight just what one's arguments are. One might spend lots of time arguing over whether the program is legal or not, but legal analysis cannot tell us whether it is a good thing to do overall, and it cannot tell us what the proper scope of the law should be. One might spend lots of time arguing about the efficacy of the program, but that cannot (by itself) tell us whether the program is normatively good on balance.

Hence, as a first step I will to set out the most plausible basic argument in support of the program, or of similar programs. The basic version of the argument is one that both supporters and detractors of the metadata program (or any national security surveillance program) could accept as reasonable. The argument and its variations are valid, which is to say, that if the premises are true, then they would entail the conclusions. Disagreement about the conclusions would therefore be

---

[5] *See, e.g.*, Susan Freiwald, *Nothing to Fear or Nowhere to Hide: Competing Visions of the NSA's 215 Program*, 12 COLO. TECH. L.J. 309, 320–22 (2014); Laura Donohue, *Bulk Metadata Collection: Statutory and Constitutional*, 37 HARV. J. L. & PUB. POL'Y 757, 764 (2014).

[6] *See, e.g.*, Donohue, *supra* note 5, at 764– 65; Freiwald, *supra* note 5, at 323–27; Randy Barnett, *Why the NSA Data Seizures are Unconstitutional*, 38 HARV. J.L. & PUB. POL'Y 3, 3 (2015).

[7] "Liberty and Security in a Changing World," 104. *See also* PETER BERGEN ET AL., NEW AMERICA FOUND., DO NSA'S BULK SURVEILLANCE PROGRAMS STOP TERRORISTS? 1 (2014) (concluding that claims of efficacy "are overblown and even misleading"), https://static.newamerica.org/attachments/1311-do-nsas-bulk-surveillance-programs-stop-terrorists/IS_NSA_surveillance.pdf; Mattathias Schwartz, *The Whole Haystack: The N.S.A. Claims It Needs Access to All Our Phone Records. But is That the Best Way to Catch a Terrorist?*, NEW YORKER (Jan. 26, 2015), http://www.newyorker.com/magazine/2015/01/26/whole-haystack; Ellen Nakashima, *NSA Cites Case as Success of Phone Data-Collection Program*, WASH. POST (Aug. 8, 2013), https://www.washingtonpost.com/world/national-security/nsa-cites-case-as-success-of-phone-data-collection-program/2013/08/08/fc915e5a-feda-11e2-96a8-d3b921c0924a_story.html.

[8] JENNIFER STISA GRANICK, AMERICAN SPIES: MODERN SURVEILLANCE, WHY YOU SHOULD CARE, AND WHAT TO DO ABOUT IT, 105-06 (2017); Bryce Clayton Newell, *The Massive Metadata Machine: Liberty, Power, and Secret Mass Surveillance in the U.S. and Europe*, 10 I/S: A J. OF L. AND POL'Y FOR THE INFO. SOC'Y 481 (2014).

based on disagreement about the truth of the premises, or based on whether there is sufficient reason to believe the premises.

The basic argument is what I take to be the most plausible argument about the conditions under which mass surveillance by security agents is justified. Making the argument explicit allows for several things. First, we can see where potential objections to mass surveillance fit. Second, we can discern some important conceptual issues. Third, we can better articulate the contingent facts that would let us conclude whether surveillance of this sort is justified. I will argue that there are some important reasons to object to the bulk metadata program. I anticipate that there will be reasons for which where others would object, or will point out that my framework allows for too much (or too little) surveillance. Nonetheless, I hope that the basic argument will allow us to better pinpoint the basis of those disagreements. Using the basic argument as a roadmap, I will argue that the bulk metadata program is plausibly, but not clearly, justifiable. This is far from a clear-cut case. In this first part of the paper, I provide several reasons for the thinking that the basic argument is unsound. What follows is three versions of a single basic argument: one moderate, one strong, and one restrictive.

A. THE BASIC ARGUMENT (MODERATE VERSION):

A1 Potential attackers (PAs) use communications systems, including telephones, to communicate with other potential attackers, and government information gathering about communications by PAs is useful in discovering other PAs.

A2 Government information gathering about communications (including phone calls) by PAs will likely lead to fewer attacks and/or greater ability to prosecute successful attackers (SAs).

A3 Gathering information about all telephone calls will include information about phone calls by PAs, and hence will likely lead to fewer attacks and/or greater ability to prosecute SAs. (A1, A2)

A4 If a government activity is overall likely to lead to fewer attacks and/or greater ability to prosecute persons who successfully plot and carry out attacks, and that activity is not illegal, and that activity is not rights-violating, then it is permissible.

A5 Gathering information about all telephone calls is overall likely to lead to fewer attacks and/or greater ability to prosecute SAs. (A3)

A6 Gathering information about all telephone calls is not illegal.

A7 Gathering information about all telephone calls is not rights-violating.

A8 Therefore, gathering information about all telephone calls is permissible. (A4, A5, A6, A7)

Premise A1 is a version of the arguments offered by government actors in support of the bulk metadata program.[9] It is also plausible enough, if only because it says very little. There are some people who wish to attack important targets in the United States, they probably use communications systems (like most people), and having information about some potential attackers is plausibly useful in finding other potential attackers (either because they communicate about plans or because they have related social networks). There is plenty of room to question what counts as a *potential attacker*. Here, I take potential attacker to mean some person who has an actual desire, proclivity, and at least minimal ability to carry out a terrorist attack. That is, I do not mean *potential* in an epistemic sense (*for all we know, anyone could be an attacker*). The definition of terrorism is contested, but for our purposes here, it is sufficient to follow Primoratz, who offers the following, "the deliberate use of violence, or threat of its use, against innocent people, with the aim of intimidating some other people into a course of action they otherwise would not take."[10] Therefore, premise A1 is plausible enough and important, but not particularly interesting.

Premise A2 does substantially more work. It makes an empirical claim that posits a causal relation between information gathering and later attacks. Whether the basic argument is sound will turn on whether A2 is true and I will return to the importance of whether A2 is true below. The first part of premise A3 is trivially true; gathering information about all calls will entail gathering information about

---

[9] *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., 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 8–9 (2014) [hereinafter "PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD"].

[10] IGOR PRIMORATZ, TERRORISM: A PHILOSOPHICAL INVESTIGATION 24 (2013).

potential attackers' communications, of which there are at least some (per A1). If premise A2 is true, then A3 follows. Notice, though, that one might doubt the truth of A2 on the grounds that gathering potential attackers' communications information with all communications in an undifferentiated mass makes it less likely that we will avoid or prosecute successful attacks.

Premises A4-A7 are crucial to getting to the core of the issue about the justifiability of the program. Premise A4 makes explicit the conditions that matter: effectiveness, legality, and the role of rights (if any are at stake). I will address premises A5-A7 in more detail below.

The gist of the moderate version of the basic argument is contained in A4. The premise allows that government actors have some discretion to act within the bounds of the law, and without violating rights, if their actions are likely to do some good, in this case by stopping or prosecuting attacks. There are two other possibilities for whether or not government action is justified. One is the restrictive version of the argument. Replace A4 with the following:

A4′ Government information collection is permissible if, and only if, it is overall likely to lead to fewer attacks and/or greater ability to prosecute persons who successfully plot and carry out attacks, and that activity is not illegal, and that activity is not rights-violating.

This is not really a serious option, unless we think that government information collection is not justifiable for any other reason (e.g., administering health codes, doing historical research, or enforcing non-terrorist related criminal law).

A more important consideration is the strong version of the basic argument, which replaces A4 with the following:

A1 If a government activity is overall likely to lead to fewer attacks and/or greater ability to prosecute persons who successfully plot and carry out attacks, and that activity is not illegal, and that activity is not rights-violating, then it is obligatory for the government to pursue it.

This is a more plausible claim than the restricted version. In fact, proponents of substantial measures may think this is true; one can imagine members of security agencies saying, 'we have an obligation to do everything within our power to stop terrorist attacks.' Nonetheless, we

can leave aside the strong version for most of our discussion, because objections to the moderate version will also be objections to the strong version. If it is not permissible for the government to pursue an activity that is likely to lead to fewer attacks or greater ability to identify successful attackers, then (*a fortiori*) it also not obligatory. With the basic argument in mind, this paper now turns to the bulk metadata program.

II. THE BULK METADATA SURVEILLANCE PROGRAM

In June 2013, news organizations began publishing stories based on the now-famous leaks by former NSA analyst Edward Snowden.[11] Among the programs disclosed was the Section 215 bulk metadata surveillance program.[12] The program began shortly after the terrorist attacks on the World Trade Center and Pentagon of September 11, 2001.[13] President Bush authorized the NSA to begin collecting the content information of certain international communications and bulk metadata (or non-content data) from telephone and internet communications.[14] The president renewed this authorization every 30 to 60 days, based on a finding of an "extraordinary emergency" until 2006.[15] In May 2006, the Foreign Intelligence Surveillance Court (FISC) approved an order to collect telephone metadata records pursuant to Section 215, rather than under a presidential emergency order.[16] This FISA court-approved program is the basis of the early Snowden revelations.

---

[11] *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013, 6:05 AM), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?hpid=z1.

[12] *See* Charlie Savage et al., *U.S. Confirms That It Gathers Online Data Overseas*, N.Y. TIMES (June 6, 2013), http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html; James Ball, *Edward Snowden NSA Files: Secret Surveillance and Our Revelations So Far*, GUARDIAN (Aug. 21, 2013, 3:36 PM), https://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations.

[13] *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 9, at 37.

[14] *Id.* at 35, 37.

[15] *Id.* at 37

[16] *Id.* at 9, 45.

To understand the program and its relation to the Basic Argument and legal archetypes, it is worth starting with the statute. Section 215 of the USA Patriot Act provides as follows:

> 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…[17]

A couple things are important to note about this provision. First, its authority is broad, allowing the FBI to obtain a court order which requires others to produce "any tangible thing" in order to protect against international terrorism.[18] "Tangible thing" includes business records and documents.[19] Second, despite the top-line breadth in 18 U.S.C. 1861(a)(1), there are several limitations to orders for tangible things, namely, (1) the records sought must be "relevant to an authorized investigation,"[20] (2) investigations may not be based solely on First Amendment protected activities of United States persons,[21] and (3) the FBI must follow minimization procedures in order to limit retention, dissemination, and use of records collection.[22] The basic features of the bulk telephone metadata program align with the Section 215 authority; thus, they are worth considering in conjunction.

Within the bulk telephone metadata program, "tangible thing" means the FBI may obtain an order for any tangible thing, including business records.[23] The FISA court determined that business records include records of transactional information (or metadata) about all telephone calls handled by telephone companies.[24] Such metadata includes: the numbers dialed by phones, the numbers calling phones, the duration of calls, and the device identification information; but it does not include the call content information (which is not metadata) and the cell tower location information (which would be metadata, but was

---

17 18 U.S.C. § 1861(a)(1) (2002).
18 *Id.*
19 *Id.*
20 50 U.S.C. § 1861(b)(2)(B) (2014).
21 *Id.* at (a)(1), (a)(2)(B).
22 *Id.* at (b)(2)(D), (g).
23 *Id.* at (a)(1).
24 *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 9, at 45-46.

purportedly not collected under the program).[25] The FISA court's order required that telephone companies provide the NSA "with 'all call detail records' generated by those companies."[26] This generated such a substantial amount of information about the calls that it allowed the NSA to make a "'comprehensive' analysis of telephone communications 'that cross different providers and telecommunications networks.'"[27] The body of communications information collected was overwhelmingly from calls both placed and received within the United States.[28]

"Relevant to" means that for records to be subject to Section 215 requests there must be "reasonable grounds to believe that the [records] are relevant to" a foreign intelligence or terrorism investigation.[29] The FISA Court set a low bar for relevance. Relevance turns on whether records requested are "necessary for NSA to employ tools that are likely to generate useful investigative leads to help identify and track terrorist operatives."[30] The court accepted the following premises: first, bulk data collection is necessary to identify the much smaller subset of terrorist communications; and second, making connections among communications is likely to generate useful investigative leads that help identify and track terrorist operatives.[31] Hence, the court concluded that the bulk metadata program meets the Section 215 relevance requirement.[32] In order to ensure that the metadata for terrorist communications is included in its data, the NSA must collect all the metadata.[33] 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.[34]

---

[25] *Id*. at 21.

[26] *Id*. at 22 (quoting *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, Primary Order, No. BR 13-158 (FISA Ct. Oct. 11, 2013) at 3).

[27] *Id*. (quoting Declaration of Teresa H. Shea, Signals Intelligence Director, National Security Agency, ¶¶ 59-60, *ACLU v. Clapper*, No. 13-3994 (S.D.N.Y. Oct. 1, 2013))[hereinafter "Shea Decl."].

[28] *Id*. at 22.

[29] 50 U.S.C. § 1861(b)(2)(B) (2014) (emphasis added).

[30] *In re* Application of the Federal Bureau of Investigation for an Order requiring the Production of Tangible Things, No. BR 13-109 (FISA Ct. July 18, 2003) at 20.

[31] *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 9, at 43-46.

[32] *See id*. at 45.

[33] *Id*. at 21.

[34] *Id*. at 22.

"Minimization procedures" are another limitation to records requests, and require a minimization plan in any application for a court order under Section 215.[35] Further, under the primary order, the government is prohibited from accessing the data for any other intelligence or investigative purpose (e.g., for general law enforcement purposes).[36] Only a few people (all trained and authorized) have access to data, and even then it is accessible via query only.[37] Making a query requires an approval from a designated official that approval must be based on a "reasonable, articulable suspicion that the selection term is associated with terrorism."[38]

Upon receiving the records from phone companies, the NSA[39] ensures that the data are in a usable format, stores the records in secure repositories accessible only by secure networks, and cleans the records of unwanted data.[40] The records are initially accessible only through a querying process, whereby analysts begin with information of interest (i.e., suspected of being associated with terrorism) then query their call record database to find connections between the seed information and other records.[41] This allows analysts to find connections among individuals and groups based on their communication networks.[42] In order for an analyst to use seed information to query their database of call records, they must first receive approval from a designated official, and that approval must be based on a "reasonable, articulable suspicion that the selection term is associated with terrorism."[43] Analysts may conduct queries up to three "hops" removed from their original selection term.[44] Based on the minimization requirements, "[t]he vast majority of the records the NSA collects are never seen by any person."[45] "Only the tiny fraction of the telephony metadata records that are responsive to

---

[35] 50 U.S.C. § 1861(b)(2)(D) (2014).

[36] *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, Primary Order, No. BR 13-158 (FISA Ct. Oct. 11, 2013) at 4.

[37] *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 9, at 33 (quoting Primary Order, at 14).

[38] *Id.* at 27 (quoting Primary Order, at 7).

[39] Section 215 authorizes the FBI to make business records requests. The bulk metadata requests specify that phone companies provide the records to the NSA, though the requests are made by the FBI. *Id*. at 42-43.

[40] *Id*. at 24-25.

[41] *Id*. at 26.

[42] *See id*. at 25-26.

[43] *Id*. at 27 (quoting Primary Order, at 7).

[44] *Id*. at 28-29.

[45] *Id*. at 26 (citing Shea Decl., *supra* note 27).

queries authorized under the RAS [reasonable, articulable suspicion] standard are extracted, reviewed, or disseminated by NSA intelligence analysts, and only under carefully controlled circumstances."[46]

A. CONSTITUTIONAL QUESTIONS: MILLER AND SMITH

In addition to legal questions posed under Section 215, there is a question as to whether the metadata program was consistent with Constitutional protections—specifically whether it violated the Fourth Amendment, which provides, "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."[47]A key question in determining whether information collection is permissible under the Fourth Amendment is whether it is indeed a search (or a seizure). Because the Fourth Amendment applies only to "unreasonable searches and seizures," information that does not constitute a search will not be an *unreasonable* search.[48]

Two cases are important in answering this question with respect to telephone metadata. In *U.S. v. Miller*, officers presented a subpoena to Miller's bank because they had neither probable cause nor a warrant to conduct a search of those records.[49] The Supreme Court determined that Miller's bank records were business records held by the bank.[50] Hence, they were the *bank's* records and Miller had no Fourth Amendment claim with respect to those records. By conducting business with a bank, one voluntarily discloses information and hence "takes the risk. . .that the information will be conveyed by that person to the Government."[51]

Smith v. Maryland directly pertains to metadata. After committing a robbery, Smith made a series of phone calls to the woman he had robbed and drove past her home.[52] The woman reported the license number of the car to police, who used it to find Smith's phone number.[53] The police had the phone company install a "pen register" that

---

[46] *Id.*
[47] U.S. CONST. amend. IV.
[48] *See* Katz v. United States, 389 U.S. 347 (1967).
[49] United States v. Miller, 425 U.S. 435, 437-38 (1976).
[50] *Id.* at 440-41.
[51] *Id.* at 443.
[52] Smith v. Maryland, 442 U.S. 735, 737 (1979).
[53] *Id.*

recorded the numbers that Smith's phone dialed.[54] The information they collected provided grounds for a warrant to search Smith's home.[55] The Supreme Court determined that Smith had no reasonable expectation of privacy in the numbers he dialed.[56] As in *Miller*, the Court determined that when people dial phones they willingly share information about the numbers they are dialing and the numbers from which they are dialing.[57] Thus, they assume the risk that their information can be revealed to the government.[58] Based on *Miller* and *Smith*, it would appear that the program is consistent with the Fourth Amendment. Indeed, a federal court dismissed a plaintiff's request to enjoin the program, concluding that they were unlikely to prevail on their claims that the program violates FISA and the Fourth Amendment.[59]

B. LEGAL CRITICISMS

The features of Section 215 and the bulk metadata program make it appear plausible that the program is legal per statute and consistent with the Fourth Amendment. That is, metadata is a form of business record and hence a tangible thing. There is a sense in which requests are relevant to ongoing investigations, and there were minimization procedures in place per the FISA court's order.

There are a number of criticisms of using Section 215 as the legal basis for the bulk metadata program. One criticism is that Section 215 permits the FBI to obtain an order for business records, but under the program, it is the NSA that receives and analyzes information.[60] The Privacy and Civil Liberties Oversight Board (PCLOB) makes the case that this conflicts with the statute, for several reasons.[61] First, records sought must be relevant to an authorized FBI investigation; however, because the NSA receives the records and is indeed prohibited from sharing its analysis with the FBI, the program conflicts with a key goal of

---

54 *Id.*

55 *Id.*

56 *See id*. at 744.

57 *Id*. at 743-44.

58 *Id*. at 744.

59 ACLU v. Clapper, 959 F. Supp. 2d 724, 754 (S.D.N.Y. 2013); *see also* David S. Kris, *On the Bulk Collection of Tangible Things*, 7 J. NAT'L SECURITY L. & POL'Y 209 (2014); PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 9, at 64.

60 PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 9, at 87-91.

61 *See id*.

the statute.[62] Second, the minimization procedures under Section 215 are to be "adopted by the Attorney General" to govern the "retention and dissemination by the Federal Bureau of Investigation" of the items or information it receives."[63] The minimization procedures directed at the FBI need not apply to the NSA, and hence the FISA court could not make a finding that the FBI adopted minimization procedures are adequate.[64] Most importantly, using Section 215 to support an NSA bulk metadata program conflicts with an important justification for the statute in first place, namely that the FBI lacked necessary statutory authority to conduct its own investigations.[65] In defending the statute, the Obama Administration stated: "Section 215 was enacted because the FBI lacked the ability, in national security investigations, to seek business records in a way similar to its ability to seek records using a grand jury subpoena in a criminal case or an administrative subpoena in civil investigations."[66]

In a sense, criticizing the program based on which agency carries it out is a slight criticism, though it points to a willingness to stretch statutory language. A more significant criticism, which further pushes the law, concerns the relevance requirement. Under Section 215, a request for an order must be based on "reasonable grounds to believe that the [records] are relevant to" a foreign intelligence or terrorism investigation.[67] The FISA Court determines that the records are relevant if they are "necessary for NSA to employ tools that are likely to generate useful investigative leads to help identify and track terrorist operatives."[68] Moreover, the court has concluded that bulk data collection is necessary in order to find the terrorist communications and that making connections amongst networks would likely lead to investigative leads and help identify and track terrorist operatives.[69] Thus, the FISA court determined that the program meets the Section 215 relevance

---

62 *Id*. at 88-89.

63 *Id*. at 89-90; 50 U.S.C. § 1861(g)(1) (2014).

64 50 U.S.C. § 1861(g)(1).

65 PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 9, at 88 (quoting EXEC. OFFICE OF THE PRESIDENT, ADMINISTRATION WHITE PAPER: BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 6, n. 2 (2013) [hereinafter ADMINISTRATION WHITE PAPER]).

66 *Id*.

67 § 1861(b)(2)(B).

68 *See In re* Application of the Federal Bureau of Investigation for an Order requiring the Production of Tangible Things, No. BR 13-109 (FISA Ct. July 18, 2003) Amended Memorandum Opinion at 20.

69 *Id*. at 21.

requirement. Put differently, to ensure that the communications information of a terrorist suspect is included, the NSA was permitted to collect all metadata. Further, the court allowed that metadata may be continually collected in order to ensure that old information is retained.[70]

The PCLOB was highly critical of the government's interpretation of the relevance requirement, calling it "untenable," "dangerously overbroad," and implying that "virtually all information may be relevant to counterterrorism and therefore subject to collection by the government."[71] This criticism is based on the FISA court's finding that bulk metadata collection was necessary for creation of useful tools, "bulk collection is necessary for NSA to employ tools that are likely to generate useful investigative leads to help identify and track terrorist operatives."[72] The Southern District of New York in ACLU v. Clapper deployed a similar understanding of relevance based on the necessity of creating counterterrorism tools.[73] As the PCLOB points out, this is overbroad. Surely having all possible information about all Americans would help find terrorists, but that per the PCLOB, cannot be the basis of a relevance claim.[74]

Further, Section 215 requires that information sought must be relevant to "an authorized investigation." The FISA court's interpretation of relevance is based on the relevance of a complete dataset for any authorized investigation. This interpretation, however, belies the requirement under Section 215 that the government provide "a statement of facts" showing "reasonable grounds to believe" records are relevant to an investigation.[75] This language implies that a unique set of facts will link the records sought to some particular investigation. But the FISA court's interpretation only requires two very broad facts for any phone metadata request, "that terrorists communicate by telephone, and that it is necessary to collect records in bulk to find the connections that can be uncovered by NSA analysis."[76]

---

[70] *Id*. at 20.

[71] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 9, at 60.

[72] *Id*. at 61 (citing *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, Amended Memorandum Opinion, No. BR 13-109 (FISA Ct. Aug. 29, 2013) at 20).

[73] *See* ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013).

[74] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 9, at 62.

[75] *Id*. at 62-63.

[76] *Id*.

Still another criticism is that the constitutional authorities upon which the metadata program relies cannot support the program's scope. *Miller* involved a narrow investigation into one person's bank records, and *Smith v. Maryland* was an investigation into a robbery.[77] Each collection of third-party information was prompted by a single investigation, and the information collected was limited to that which shed light on that investigation.[78] But the bulk metadata program involves millions upon millions of individuals' records, collected through tools much more sophisticated than those available and used when *Smith* and *Miller* were decided.[79] The vast number of records collected allows many more people to be investigated (indeed, potentially anyone communicating with a cell phone on the networks subject to the orders during the period in which the program has operated).[80] Indeed, the PCLOB and the District Court for the District of Columbia have argued that the program pushes against constitutional limits.[81] The Board emphasized the "rapid technological changes and in light of the nationwide, ongoing nature of the program" as key differences between the program and *Smith*.[82]

In *Klayman v. Obama*, the District Court for the District of Columbia granted a preliminary injunction against the program based on Fourth Amendment concerns.[83] The court also emphasized that bulk metadata collection is a far cry from the pen register in *Smith*.[84] Instead, the court turned to *U.S. v. Jones*, where the Supreme Court held that police placing a GPS device on a car for several weeks was a search.[85] Concurring in *Jones*, Justice Sotomayor distinguished between long-term monitoring and more isolated information gathering, allowing constant following via GPS could constitute a search; even where discrete elements of that following would not.[86] Following *Jones*, the D.C. court determined that bulk metadata collection could constitute a search even where discrete collection of metadata would not.[87]

---

[77] Smith, 442 U.S. 735, 737-38; Miller, 425 U.S. 435, 436-38.

[78] *See generally* Smith, 442 U.S. at 737; Miller, 425 U.S. at 438.

[79] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 9, at 127.

[80] *See id*. at 114.

[81] *Id.*; *see* Klayman v. Obama, 957 F. Supp. 2d 1 (D.C. Cir. 2013).

[82] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 9, at 114.

[83] *Klayman*, 957 F. Supp. 2d at 43.

[84] *Id*. at 31-32.

[85] U.S. v. Jones, 565 U.S. 400, 406-07 (2012) (slip op.).

[86] *Id*. at 413-31 (Sotomayor, J. concurring).

[87] *Klayman*, 957 F. Supp. 2d at 37.

C. THE USA FREEDOM ACT

In June 2015, Congress passed, and the president signed into law, the USA Freedom Act.[88] The legislation was inspired by the controversy surrounding the bulk metadata program, and makes important modifications to the business records provisions upon which the program was based.[89] The Freedom Act performs several specific functions. First, perhaps most importantly, it requires that FBI applications for orders for the production of tangible things be based on a specific selection term.[90] As such, the production of all call detail records in bulk is not permissible under this provision. Second, it allows information to be collected from up to two "hops" from the specific selection term.[91] Third, the Act limits what kinds of business records may be collected.[92] It specifically excludes communications content—names, addresses, and financial information of subscribers—and location information (GPS or cell tower information).[93] Fourth, the act requires the FISA court order approving the production of tangible things to include selection terms.[94] The Act also includes FISA court related changes, in particular establishing amicus curiae to help review legality of records collection and other matters.[95] It also makes publicly available any significant new constructions and interpretations of law.[96]

In sum, the bulk metadata program is plausibly legal, though the interpretations of the statutes are aggressive and push against the limits of the statutory language. The program is also plausibly consistent with important Fourth Amendment cases, though that too is an uneasy fit. The USA Freedom Act may address some of these concerns; I will revisit that in Part IV.

---

88 Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act of 2015, Pub. L. No. 114-23, 129 Stat. 268.

89 *See id*.

90 *Id*. at § 103.

91 *Id*. at § 101.

92 *Id*. at § 107.

93 *Id*.

94 *Id*. at § 103.

95 *Id*. at § 401.

96 *Id*. at § 402.

III. THE BASIC ARGUMENT REVISITED

Let us return to the Basic Argument. As the basic argument makes clear, the legality of the metadata program is a necessary condition for its permissibility. The mere fact that the program is legal does not entail that the law is as it should be. Moreover, the laws relevant here—the Patriot Act §215 and the Fourth Amendment—create a legal permission conducting surveillance under certain conditions.[97] The laws do not create a positive obligation to act. Surveillance is discretionary and there remains a question of when exercising that discretion is justified. The bulk of the basic argument is meant to answer that question.

Premise A4 states that if: (1) a government activity is overall likely to lead to fewer attacks or a greater ability to prosecute persons who successfully plot and carry out attacks, (2) that activity is not illegal, and (3) that activity is not rights-violating; then it is permissible. The crux of premise 4 is that it sets out a familiar juxtaposition between consequences and rights. On the one hand, it takes into account the consequences of a government action and posits that when the consequences of that action are beneficial overall, it is permissible (absent rights violations and illegality). Coupled with premise A5—that bulk metadata collection will lead to fewer attacks or prosecution for attacks—we get a conclusion about the overall consequences of metadata collection. But is premise A4 true?

In "Security and Liberty: The Image of Balance," Jeremy Waldron addresses the idea that, in light of terrorist threats, the US and other Western democracies must strike a "balance" between security and liberty.[98] Waldron interprets this notion of balance to be an implicit adoption of consequentialism.[99] The argument is as follows, because we have become aware of greater threats to physical well-being, and on the assumption that close adherence to certain civil liberties make the likelihood of those threats greater, it will lead to better consequences to have less protection for those civil liberties.[100] As Waldron points out, at least some goods are not important based solely on consequences.[101] For

---

[97] 50 U.S.C. § 1861(a)(1) (2002).

[98] *See* Jeremy Waldron, *Security and Liberty: The Image of Balance*, 11 J. POLITICAL PHIL., no. 2, 2003, at 191.

[99] *Id*. at 194–95 .

[100] *Id*. at 195–96.

[101] *Id*. at 196–97.

example, rights to free speech, conscience, association, due process, and so forth are on many conceptions not based on the good consequences that result.[102] For this reason, premise A4 allows that government activity leading to good consequences is not permissible where there are rights violations.

Even if we set aside the argument that better consequences alone do not suffice to override rights, there is a question of just what consequences count. Premise A4 recognizes the negative consequences of terrorist attacks and the positive consequences of government activity that can help thwart those attacks. This seriously undercounts the potential negative consequences. Waldron's "Image of Balance" provides further guidance here. In discussing what outcomes are relevant in determining whether curtailing civil liberties is justified, he points to the traditional apprehension of state power found in liberal political theory:

> [A]n increase in the power of the state may be necessary to prevent or diminish the prospect of that horror [of catastrophic terrorist attacks]. But the existence of a threat from terrorist attack does not diminish the threat that liberals have traditionally apprehended from the state…We have to worry that the very means given to the government to combat our enemies will be used by the government against its enemies—and although these two classes "enemies of the people" and "enemies of the state" overlap, they are not necessarily co-extensive.[103]

The idea is a familiar one, but worth keeping in mind. There is no question that terrorist threats are real, and that the NSA and other security and law enforcement agents aim to diminish those threats. Any government agency can also mischaracterize or misinterpret persons opposed to the government, or doing something that the government does not like, as being threats to people generally. Consider the murky case of Snowden himself. One possibility is that Snowden's actions have actually made people in the United States and elsewhere more vulnerable to attack. He is also deeply embarrassing to the US government, to national security agencies, and to national security contractors. It is reasonable to interpret the government's enthusiasm in apprehending and discrediting Snowden as based on mixed motives and including an

---

[102] *Id.*; *see also* Joseph Raz. *Practical Reason and Norms*, 37 (1999); Robert Nozick, *Anarchy, State and Utopia*, 28 (1974).

[103] Waldron, *supra* note 98, at 205–06.

element of score settling on behalf of the government, agencies, and contractors.

What dangers loom from metadata gathering? It is difficult to know for certain, but there are several dangers we can consider. The most important, is the potential for misuse of intelligence. As the PCLOB stated, "An even more compelling danger is that personal information collected by the government will be misused to harass, blackmail, or intimidate, or to single out for scrutiny particular individuals or groups."[104] The board describes a number of cases of improper searching.[105] These do not appear to be intentional.[106] Nonetheless, the wrongs of that kind of abuse are particularly acute; it is not merely the bad consequences that result, but the violation of official capacities and trust.

Based on this idea, we need to modify premise A4 of the basic argument as follows:

A4″ If a government activity is overall likely to lead to fewer attacks and/or greater ability to prosecute persons who successfully plot and carry out attacks, and does not create other threats of similar (or greater) magnitude, and that activity is not illegal, and that activity is not rights-violating, then it is permissible.

We also need to add an additional premise to the basic argument to make it valid:

A9 Gathering information about all telephone calls does not create threats that are as likely and of similar magnitude as the threats that the surveillance thwarts.

As noted in the previous section, premise A4 recognizes the importance of both the consequences of government activity and rights, and avoids reducing respect for rights to an exercise in maximizing welfare. Therefore, an activity may be impermissible if it either fails to generate overall better consequences or it impinges rights. In addition, as noted in the previous section, there are at least some reasons to be suspicious that the consequences are on balance positive. First, it is unclear how

---

[104] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *supra* note 9, at 12.
[105] *Id.* at 47–56.
[106] *Id.* at 12.

substantial the positive consequences of mass metadata collection are.[107] Second, the potential negative consequences of government surveillance tend to be undercounted.[108]

Suppose that on balance there are benefits to the surveillance. Perhaps it substantially decreases the likelihood of attacks and it does not entail large opportunity costs, and that there are enough checks in place to guard against state power.[109] The question then is whether there are other considerations that would render the program unjustified. As premise A4 entails, the existence of some right could do so; though premise A7 states that the program does not infringe rights. Elsewhere I have argued that the Section 215 program does infringe privacy rights, though those infringements are limited.[110] Nevertheless, for the sake of argument here, suppose there is not an individual right that is violated by the collection of metadata. That is, assume, for the sake of reaching the question of legal archetypes below, that bulk metadata collection cannot be wrong based on a series of rights violations on the grounds that there is no such individual right.

IV. LEGAL ARCHETYPES

So what's left? Here I want to return to premise A4:

A4″ If a government activity is overall likely to lead to fewer attacks and/or greater ability to prosecute persons who successfully plot and carry out attacks, and does not create other threats of similar (or greater) magnitude, and that activity is not illegal, and that activity is not rights-violating, then it is permissible.

---

[107] *See* Waldron, *supra* note 98, at 207–08.

[108] *Id.*

[109] Consider the conclusions of the Presidents Group on Intelligence and Communications Technologies: "the information contributed to terrorist investigations by the use of Section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional Section 215 orders." "Liberty and Security in a Changing World," EXEC. OFFICE OF THE PRESIDENT, LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 104 (Dec. 12, 2013). *See also* Peter Bergen, David Sterman, Emily Schneider, & Bailey Cahall, *Do NSA's Bulk Surveillance Programs Stop Terrorists*, 1 (Jan. 2014)(concluding that claims of efficacy "are overblown and even misleading.").

[110] Alan Rubel, *Privacy Transparency, and Accountability in the NSA's Bulk Metadata Program, in* PRIVACY, SECURITY, AND ACCOUNTABILITY 183–202 (Adam Moore ed., 2015).

In particular, I want to consider the issue of "not illegal." The ambiguity in that phrasing is important. As discussed Part II, the PCLOB found substantial fault in the legal reasoning of the FISA court, because the issuing orders for phone metadata pushed "relevance" beyond what the concept could hold and ignored the statute's specification that the FBI (rather than the NSA) obtain an order for tangible things. At least one federal court has suggested that the program impermissibly extended what could be allowed under the Fourth Amendment.[111]

In "Torture and Positive Law: Jurisprudence for the White House," Jeremy Waldron argues that some legal rules operate in law as principles that go beyond a narrow articulation in statutes and constitutional provisions.[112] These are pervasive principles or *legal archetypes*.[113] Waldron's target is the legal wrangling that sought to justify torture by the United States in the aftermath of September 11, 2001. His argument takes as a starting point the three defining currents in the debates about whether suspected terrorists could be subjected to torture.[114] The first is a 2002 memo authored by John Yoo arguing that the United States should not recognize Geneva Convention protections for prisoners from Al Qaeda and the Taliban.[115] The Yoo memo argued that members of Al Qaeda and the Taliban were not protected because the *type* of armed conflict in which they were involved was not explicitly protected in the Geneva Conventions.[116] The second defining current is the publications of Alan Dershowitz, a law professor at Harvard. Dershowitz argued that torture was morally justified on consequentialist grounds, and that there should be a legally recognized procedure (judicial warrants) underwriting particular instances of torture that are likely have substantial beneficial consequences.[117] The third is a memorandum signed by Jay Bybee (then head of the Office of Legal Counsel in the US Department of Justice) narrowing the definition of 'torture' so that it

---

[111] Klayman v. Obama, 957 F. Supp. 2d 1 (D.C. Cir. 2013).

[112] *See* Jeremy Waldron, *Torture and Positive Law: Jurisprudence for the White House*, 105 COLUM. L. REV. 1681 (2005).

[113] *Id*.

[114] *Id*. at 1684–86.

[115] *Id*. at 1684 (citing U.S. Dept. of Justice, Off. of Legal Couns., Memorandum of John Yoo and Robert Delahunty for William J. Haynes II regarding the Application of Treaties and Laws to Al Qaeda and Taliban Detainees (Jan. 9, 2002)) [hereinafter "Yoo Memo"].

[116] *Id.* at 1685 (citing Yoo Memo, at 11–25).

[117] *Id*. at 1685 (citing ALAN DERSHOWITZ, SHOUTING FIRE: CIVIL LIBERTIES IN A TURBULENT AGE 470–77 (2002)).

excluded many cases of the deliberate infliction of pain.[118] Specifically, the memo argued that torture included only inflicting the degree of pain associated with organ failure or death.[119]

Waldron's concern is not that these legal moves in support of torture are (ipso facto) in support of something that is morally prohibited. Rather, it is that they seek to place a legal imprimatur on torture.[120] They narrowly parse legal language (in the case of the Yoo and Bybee memos) or normalize torture within legal procedure (the arguments for torture warrants).[121] Exacting treatment of legal language and creation of procedures to avoid ad hoc rules is what lawyers often do. In Waldron's view, however, it is inappropriate in some cases because doing so contradicts legal principles, viz cases involving legal archetypes.[122] According to Waldron, because torture is such an archetype, the torture memos and articles by Yoo, Bybee, and Dershowitz are unjustifiable.[123]

Waldron's understanding of legal archetypes shows how premise A4 of the basic argument is incomplete. Premise A4 focuses on government activity that has positive consequences, is not rights-violating, and which is *not illegal*. Nevertheless, Waldron's sense of archetypes carves out a conceptual space between the moral considerations of rights and consequences and the legal space. Legal archetypes are principles that are part of law, even if they are not explicitly articulated in statutes and constitutions.

The importance of legal archetypes is that they are engrained as part of the law so undermining them will damage the larger body of law itself.

> When I use the term "archetype," I mean a particular provision in a system of norms which has a significance going beyond its immediate normative content, a significance stemming from the fact that it sums up or makes vivid to us the point, purpose, principle, or policy of a whole area of law. Like a Dworkinian principle, the archetype performs a background function in a given legal system. But archetypes differ from Dworkinian principles and policies in that they *also* operate as foreground provisions. They work in the

---

[118] Waldron, *supra* note 112, at 1685.

[119] *Id*. at 1685 (citing U.S. Dept. of Justice, Off. of Legal Couns., Memorandum of Jay S. Bybee for Alberto R. Gonzales regarding the Standards of Conduct for Interrogation under 18 U.S.C. §§ 2340-2340A (Aug. 1, 2002)).

[120] *Id.* at 1735.

[121] *Id*. at 1694, 1706–07, 1716.

[122] *Id*. at 1735.

[123] *Id*. at 1734–39.

> foreground as rules or precedents, but in doing so, they sum up the spirit of a whole body of law that goes beyond what they might be thought to require on their own terms. The idea of an archetype, then, is the idea of a rule or positive law provision that operates not just on its own account, and does not just stand simply in a cumulative relation to other provisions, but operates also in a way that expresses or epitomizes the spirit of a whole structured area of doctrine, and does so vividly, effectively, and publicly, establishing the significance of that area for the entire legal enterprise.[124]

Waldron is drawing on a key thread of analytic jurisprudence over the past several decades. Specifically, he is referencing Ronald Dworkin's "Model of Rules I."[125] There, Dworkin distinguishes between legal rules and legal principles.[126] Legal rules are rules which when they operate are dispositive.[127] That is, rules are "all-or-nothing," when they apply they provide a unique answer to a legal case. In contrast, legal principles are, as Michael Plaxton puts it, "the background motivations and reasons which justify the creation and existence of the specific rules in a legal system."[128] Legal principles, according to Dworkin, are part of law itself.[129] They are not moral principles about what law should be, but principles built into law itself that are instantiated in the positive law of statutes, cases, constitutions, administrative rules, and other facets of positive law.

Waldron's understanding of archetypes is, per Plaxton, "a hybrid of rules and principles."[130] The archetype is iconic or emblematic because it makes clear the reason for the existence of certain sets of legal rules. In the case of archetypes, the specifics of legal rules are the background; they matter less than the deeper, moral justifications for those rules. As the specific legal rules instantiate those moral justifications, those justifications are part of law itself.[131] So, by way of example, Waldron argues that what is important about *habeas corpus* statutes is not their precise content—though, of course, procedure matters—rather, it is that *habeas corpus* statutes as a whole are justified by, embody, and make vivid the deeper moral fact that persons should never be confined

---

[124] *Id*. at 1723.
[125] *See* Ronald M. Dworkin, *The Model of Rules*, 35 U. CHI. L. REV. 13 (1967).
[126] *Id*. at 22–23.
[127] *Id*. at 25.
[128] Michael Plaxton, *Reflections on Waldron's Archetypes*, 30 L. & PHIL., no. 1, 2011, at 77, 80.
[129] *See* Dworkin, *supra* note 125, at 22–23.
[130] Plaxton, *supra* note 128, at 81.
[131] Waldron, *supra* note 112, at 1723.

arbitrarily.[132] Similarly, Waldron draws on the case of *Brown v. Board of Education* to demonstrate archetypes:

> In itself, *Brown v. Board of Education* is authority for a fairly narrow proposition about segregation in schools, and its immediate effect in desegregation was notoriously slaw and limited. But its archetypal power is staggering: In the years since 1954 it has become an icon of the law's commitment to demolish the structures of de jure (and perhaps also de facto) segregation and to pursue and discredit forms of discrimination and badges of racial inferiority wherever they crop up in American law or public administration.[133]

The focus on the narrow language and specific legal rule articulated in *Brown* misses the deeper significance of the ruling as being justified by and embodying a deeper, moral value of non-discrimination. Suppose, for example, that a court made a narrow, language-parsing argument that some forms of educational discrimination were permissible (despite *Brown*). They might abide language of *Brown* while undermining the legal archetype of non-discrimination.

Waldron's target is torture. He argues that rules against torture (be they based on Geneva Conventions, or statutes defining what torture is) are "archetypal of a certain policy having to do with the relation between law and force, and the force with which law rules."[134] Even though governing by law deploys physical force, it ought not deploy force brutally, "Law is not brutal in its operation. Law is not savage. Law does not rule through abject fear and terror, or by breaking the will of those whom it confronts."[135] Now, of course *uses* of the law may be brutal, just as uses of the law may arbitrarily detain people or discriminate on the basis of race. Such uses, however, are wrong and the rules against torture, of habeas corpus, and against discrimination instantiate and make vivid the deeper principles that render those uses wrong. Hence, it is not merely that torture (or *habeas corpus*, or equal protection) laws are justified by underlying moral principles, but when such laws instantiate such principles, the principles themselves may be archetypes. The problem Waldron sees in the Yoo and Bybee memos, which narrowly parse who is subject to torture prohibitions and whether torture is limited to injury that tends to lead to organ failure or death, is that such parsing undermines the legal archetype that torture statutes

---

[132] *Id*. at 1724.
[133] *Id*. at 1725 (citing Brown v. Board of Education of Topeka, 347 U.S. 483 (1954)).
[134] *Id.* at 1726.
[135] *Id.*

instantiate. The problem with Dershowitz's arguments for torture warrants is that it would be a legally cognizable instrument directly contradicting those archetypes. Again, as Plaxton explains where legal archetypes are in play, lawyers are responsible for interpreting them broadly so as not to cut it close at all:

> [T]here is something wrong with trying to pin down the prohibition on torture with a precise legal definition. Insisting on exact definitions may sound very lawyerly, but there is something disturbing about it when the quest for precision is put to work in the service of a mentality that says, "Give us a definition so we have something to work around, something to game, a determinate envelope to push."[136]

Two further features of archetypes are relevant here. Waldron writes that his claim regarding archetypes has two aspects. First, there must be a "body of law in question [which] is pervaded by a certain principle or policy." Second, the provision in question must be archetypal of that policy or principle in that it renders lesser violation inconsequential.[137] Note that this second feature is *not* a slippery slope argument. It is not that violation of an archetype makes additional, more consequential violations easier. Rather, it is that the violation of the archetype makes *lesser* violations more palatable. Hence, violating torture archetypes will make less severe forms of brutality (harsh treatment upon arrest, minor and arbitrary deprivations) seem routine or small beer. Indeed, Waldron emphasizes that this is the reverse of slippery slope; rather than being at the top and likely to slip to the bottom, undermining an archetype is staking out territory at the bottom of a slope, such that points further up appear better by comparison.[138]

So, we come to the crux of the argument: whether the bulk metadata program undermines a legal archetype. Premise A4 of the basic argument, again, allows that surveillance programs are permissible when (1) they have good consequences (i.e., lead to fewer attacks or greater ability to prosecute persons who successfully plot and carry out attacks), (2) are not rights-violating, and (3) are *not illegal*. But Waldron's understanding of legal archetypes shows that this premise contains an ambiguity. The question for surveillance becomes whether the bulk metadata program violates a legal archetype. I would argue that it does

---

[136] *Id*. at 1687; *see also* Plaxton, *supra* note 128, at 84.

[137] Waldron, *supra* note 112, at 1729.

[138] *Id*. at 1735.

and to make the case I will first, articulate what the archetype is, and then the body of law that is pervaded by that principle. Next, I will show that the provision in question (here the bulk metadata program) is an archetypal violation in that it renders lesser violations inconsequential.

First, what is the archetype? The most plausible case is the idea of individualized suspicion. Persons in the United States must be investigated and have their information deliberately collected for reasons that are traceable *to that person*. I believe this idea is indeed an archetype, such that there is a body of law pervaded by that principle, for several reasons. First, at the broadest level the Fourth Amendment protects against "unreasonable" searches and seizures, and requires that warrants will be issued only where there is probable cause—some degree of individualized suspicion.[139] That individualized suspicion is built into the Constitution is a good foundation for a legal archetype. The argument is that there is a moral value *embodied in* the Fourth Amendment that constitutes an archetype. Second, there are a number of Fourth Amendment cases that recognize the need to be wary of technological encroachments on privacy.[140] These cases include *Jones*, discussed above, where the Supreme Court determined that attaching a GPS unit to a car and tracking it for weeks constituted a search, and a concurrence maintained that amassing lots of data may itself violate a constitutional right (even if collection of a smaller amount of data may have been permissible.)[141]

The final criterion for Waldron's archetypes is whether the program renders lesser violations inconsequential. This is the crux of the matter. In the case of torture, one of Waldron's key concerns is that narrow parsing of legal language so as to allow brutal treatment that ought to fall under torture prohibitions will make lesser forms of brutality seem tame by comparison, and hence less likely to be restricted or abhorred. A similar concern is warranted in the case of bulk metadata collection. Once the NSA has gathered metadata in bulk, smaller (though still pervasive) collections of communications information hardly seem so bad. Indeed, the hard-fought and important legal victory of the passage of the USA Freedom Act still allows collection of metadata from selection terms, and collection of metadata two "hops" away from those

---

[139] U.S. CONST. amend. IV.

[140] *See generally* Katz v. United States, 389 U.S. 347, 347 (1967); United States v. Karo, 468 U.S. 705 (1984); Kyllo v. United States, 533 U.S. 27 (2001); Florida v. Jardines, 133 U.S. 1409 (2013) (Kagan, J., concurring); Riley v. California, 134 U.S. 2473 (2014).

[141] U.S. v. Jones, 565 U.S. 400, 412–17 (2012) (Sotomayor, J., concurring).

terms.[142] That is still intrusive, and perhaps in accord with what people thought was originally allowable under the Section 215. Moreover, gathering of metadata by other law enforcement and security agencies, even on a limited basis, does not seem to raise an eyebrow.

It is worth pausing here to recognize that the argument that the bulk metadata program undermines legal archetypes need not depend solely on US statutory and Constitutional law. The idea of a legal archetype turns on the concept of law, and principles that inhere in law even where not explicit. Hence, while the arguments so far have addressed the particular program at work in the United States and legal archetypes that inhere in US law, there is reason to think that similar archetypes inhere in other law and that data collection programs may conflict with those as well.

Consider two recent issues before the United Kingdom's Investigatory Powers Tribunal (IPT), both advanced by the nongovernmental agency Privacy International.[143] The first involves a challenge to computer hacking conducted by Government Communications Headquarters ("GCHQ"). Among the Snowden revelations was information that GCHQ had participated in NSA-initiated programs and had substantial surveillance operations with comparatively light oversight.[144] In a report of the UK Investigatory Powers Review ("A Question of Trust"), David Anderson, QC describes several examples of what Privacy International calls computer network exploitation, or CNE:

> Examples in the documents describing the use of this technique by GCHQ included a programme called NOSEY SMURF which involved implanting malware to activate the microphone on smart phones, DREAMY SMURF, which had the capability to switch on smart phones, TRACKER SMURF which had the capability to provide the location of a target's smart phone with high-

---

[142] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act of 2015, Pub. L. No. 114-23, § 101, 129 Stat. 268, 269–71.

[143] Privacy International v. Greennet, Ltd. [2016] UKIP 14_85 CH (U.K.).

[144] *See generally* Ewan MacAskill, Julian Borger, Nick Hopkins, Nick Davies & James Ball, *The Legal Loopholes that Allow GCHQ to Spy on the World*, THE GUARDIAN (June 21, 2013), https://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world; Nick Hopkins, *UK Gathering Secret Intelligence via Covert NSA Operation*, THE GUARDIAN (June 7, 2013), https://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism.

> precision, and PARANOID SMURF which ensured malware remained hidden.[145]

Privacy International filed a legal complaint with the Investigatory Powers Tribunal (IPT), and seven internet service providers filed similar complaints.[146] The tribunal determined that the programs were lawful and consistent with Articles 8 and 10 of the European Convention on Human Rights.[147] Privacy International has sought review of the tribunal's decision in the UK Administrative Court. [148] What is important for the purposes of this paper is that Privacy International's arguments are similar to the archetype arguments that Waldron raises in the context of torture and that I have outlined here.

Among the key issues in *Greennet* was whether section 5 of the United Kingdom's Intelligence Services Act of 1994 authorizes the kind of broad computer network exploitation revealed in Snowden's leaks and in "A Question of Trust." Section 5(2) states that

> The Secretary of State may, on an application made by the Security Service, the Intelligence Service or GCHG, issue a warrant under this section authorizing the taking. . .of such action as is specified in the warrant in respect of any property so specified or in respect of wireless telegraphy so specified. . .

While Privacy International maintained that the most plausible construction of Section 5 requires warrants specify persons or properties, they also held that common law "sets its face against general warrants," and that thus the IPT should conclude that no warrant could allow the broad CNE that GCHQ had been conducting.[149] The government argued that the use of "specified" in the statute does not require specification of persons, locations, or properties. Rather, all that is required is "the best description possible."[150] The IPT agreed with the government.[151]

In its claim seeking review of the IPT decision, Privacy International argues that cases prohibiting general warrants are grounded

---

[145] DAVID ANDERSON, Q.C. A QUESTION OF TRUST: REPORT OF THE INVESTIGATORY POWERS REVIEW 332 (June 2015), https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf.

[146] *See generally Greennet*, UKIP 14_85 CH.

[147] *Id*. at ¶ 89.

[148] *Id*. at Statement of Facts and Grounds (citing Money v. Leach (1765), 3 Burr 1742 and Wilkes v. Wood (1763) Lofft 1).

[149] *Id.* at ¶ 35.

[150] *Id*. at ¶ 36.

[151] *Id*. at ¶ 37.

in deeper principles that ought not be abandoned by permissive interpretations of statutes.[152] In support, it cites several classic common law cases antithetical to general warrants.[153] Moreover, Privacy International relies on Article 8 of the European Convention on Human Rights, which states, "Everyone has the right to respect for his private and family life, his home and his correspondence."[154] The important thing about Privacy International's claims is that the principles it adduces are principles that are part of law (common law cases, the ECHR) which do not bear directly on the statutory language at issue in *Greennet*. Rather, the cases and ECHR together establish a legal archetype— a "provision in a system of norms which has a significance going beyond its immediate normative content, a significance stemming from the fact that it sums up or makes vivid to us the point, purpose, principle, or policy of a whole area of law."[155] The IPT's permissive reading of "specified" would thus undermine that archetype.

The second recent case concerns use of Bulk Personal Datasets (BPDs) and Bulk Communications Data (BCD) by various security and intelligence agencies in the United Kingdom (including GCHQ, MI5, and MI6).[156] In 2015, the UK government acknowledged that since 2001, GCHQ had been collecting and using BCD under section 94 of the United Kingdom's Telecommunications Act of 1984,[157] and MI5 avowed section 94 collection and use of BCD.[158] In addition, in 2015, those agencies, along with MI6, disclosed collection and use of BPD under a range of authorities.[159] The Investigatory Powers Tribunal determined that collection of BCD was consistent with the authority granted in Section 94.[160]

---

[152] *Id.* at ¶ 6 (citing Entick v. Carrington (1765) 2 Wilson KB 275, Money v. Leach (1765) 3 Burr 1742 and Wilkes v. Wood (1763) Lofft 1).

[153] *Id.* at ¶ 6 (citing Entick v. Carrington (1765) 2 Wilson KB 275 (establishing that exercise of power of public officials to search a house requires specific statutory or common law regime), Money v. Leach (1765) 3 Burr 1742 (prohibiting use of general warrants that neither name nor describe a person to seize a person), and Wilkes v. Wood (1763) Lofft 1)(prohibiting use of general warrant to seize papers)).

[154] European Convention on Human Rights, art. 8, Nov. 4, 1950, 213 U.N.T.S. 262.

[155] Waldron, *supra* note 112, at 1723.

[156] *See generally* Privacy International v. Secretary of State for Foreign and Commonwealth Affairs [2016] UKIP 15_110 CH (U.K.).

[157] *Id.* at ¶ 10.

[158] *Id.*

[159] *Id.* at ¶¶ 6–7, 13-15.

[160] *Id.* at ¶ 58.

The IPT also considered whether the BCD and BPD regimes were consistent with Article 8 of the ECHR, in particular the requirement that "[t]here shall be no interference by a public authority with the exercise of this right [to private and family life] except such as is in accordance with the law."[161] The tribunal based this determination on, first, the secrecy of programs, stating "[I]t seems difficult to conclude that the use of BCD was foreseeable by the public when it was not explained to parliament."[162] Second, it pointed to the lack of oversight, stating, "[W]e are not satisfied that, particularly given the fragmented nature of the responsibility apparently shared between the Commissioners, there can be said to have been an adequate oversight of the BCD system."[163] As such, it concluded that the programs were inconsistent with Article 8 at times prior to the government's avowal of their existence, though consistent with Article 8 after avowal.

The IPT's decision comports with some of Privacy International's grounds for complaint in the case. In particular, Privacy International argued, "The acquisition, retention and use of a large database of information or the use of a national security direction to accumulate or intercept personal data plainly amounts to a serious interference with the Article 8 right of privacy."[164] Privacy International argues, Article 8's requirement that interference with private and family life be "in accordance with the law," means that such interference must be "compatible with the rule of law."[165] The idea is again similar to that of legal archetypes. Specifically, that there are legal principles that are part of law, even if not explicitly articulated in statutes and constitutions themselves. The requirement that use of statutory provisions (such as Section 94) be compatible with rule of law cannot in principle be articulated *in* a statute or constitution because rule of law is a precondition for statutes and constitutions to *be* law. Hence, invoking Article 8 to criticize the United Kingdom's BCD and BPD programs appears to be an appeal to legal archetypes.

---

[161] European Convention on Human Rights, art. 8, § 2, Nov. 4, 1950, 213 U.N.T.S. 262.

[162] Privacy International v. Greennet, Ltd. [2016] UKIP 14_85 CH (U.K.), ¶ 70.

[163] *Id*. ¶ 80.

[164] *Privacy International*, UKIP 15_110 CH, at ¶ 23.

[165] *Id*. at ¶ 24 (quoting Gillan v. United Kingdom (2010) 50 EHRR at § 76).

V. CONCLUSION

In conclusion, this paper proposes the most plausible basic argument for security-based surveillance. Such surveillance is plausibly justifiable where the consequences are positive, where it is not rights violating, and where it is not illegal. The bulk metadata program is a hard case. It is *plausibly* legal insofar as it turns on aggressive interpretations of statutes and permissive interpretations of relevant Fourth Amendment law. The effort to push law so far makes vivid an ambiguity in the "not illegal" requirement. I have argued that Waldron's conception of legal archetypes illustrates that ambiguity. Narrow parsing of legal language in some cases may provide a rationale for actions, but if it is done in contradiction of legal archetypes it undermines an important facet of law. In other words, pushing legal language to its limits may undermine principles embodied in law. Where doing so undermines an important archetypal facet of law, and makes lesser violations inconsequential, it is impermissible. That is not quite a legal issue, and it is not strictly a moral issue. Rather, it is both. I have suggested that the metadata program does affect a legal archetype, and that surveillance conducted under the USA Freedom Act will appear inconsequential as a result. It will be difficult for us to discern whether its appearing inconsequential is because it *is* inconsequential or because it appears so in comparison to the bulk metadata program.

Now there are many ways to object to this argument. One is that the *real* argument about surveillance should take place in regards to whether programs are effective, or in regards to rights. One might instead argue that the real issues lie not in this moral talk, but in the law itself. Perhaps it just is the case that the program violates statutes or conflicts with the Fourth Amendment, and that addressing legal archetypes is just a way to smuggle something into the law that is not there. While those are important objections, my task here has been to try to meld them. The law does embody values (whether they are good ones or not is always a ripe debate), and the fact that it embodies values provides reason to respect law. Waldron's archetypes are one way to understand that relation between law and morality, and in the end I think they are useful in thinking through these more difficult questions where legal interpretations may conflict with values that a body of law instantiates.