I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

The Massive Metadata Machine: Liberty, Power, and ~~Secret~~ Mass Surveillance in the U.S. and Europe

BRYCE CLAYTON NEWELL*

Abstract: This paper explores the relationship between liberty and security implicated by secret government mass surveillance programs. It includes both doctrinal and theoretical analysis. Methodologically, the paper examines judicial reasoning in cases where parties have challenged secret government surveillance programs on Constitutional or human rights grounds in both United States' Courts and at the European Court of Human Rights (ECtHR). Theoretically, this paper will draw on theories in the fields of law, surveillance studies, and political theory to question how greater recognition of citizen rights to conduct reciprocal surveillance of government activity (for example, through expanded rights to freedom of information) might properly balance power relations between governments and their people. Specifically, the paper will question how liberal and neorepublican conceptions of liberty, defined as the absence of actual interference and the possibility of arbitrary domination, respectively, and the jurisprudence of the ECtHR can inform the way we think about the proper relationship between security and liberty in the post-9/11, post-Snowden United States of America.

---

* Ph.D. Candidate, University of Washington (Seattle), Information School; M.S. in Information Science, University of Washington; J.D., University of California, Davis School of Law. The author especially wishes to thank Stephen M. Gardiner, Adam D. Moore, Alan Rubel, and Peter Shane for their helpful comments, suggestions, and critiques of the arguments presented herein. Additional thanks are due to Laura Lenhart, Chris Heaney, Nicole Cunningham, Kai Chi (Sam) Yam, and the participants of the pre-conference workshop at the 2013 Information Ethics Roundtable in Seattle, Washington, who all provided valuable feedback on some aspects of the overall development of this paper's primary arguments.

I. INTRODUCTION

Information can provide and facilitate power. As such, the collection and use of large amounts of information (including communications metadata) can significantly impact the relationships between governments and their citizens.[1] Access to information is also often a prerequisite to exercising power or seeking redress for potential rights violations stemming from secret activities of others.[2] As such, an imbalance in information access between a people and their government can tip the scales of power and limit the ability of the people to exercise democratic oversight and control those they have put in power to represent them.[3] Freedom of information (FOI) laws often provide a great deal of access to government records and serve as a powerful and effective means for empowering oversight by journalists and ordinary citizens. In a very real sense, these laws provide a legal mechanism for citizen-initiated surveillance from underneath (sometimes termed "sousveillance"[4] or the "participatory panopticon"[5]). This form of reciprocal surveillance (which may take numerous forms) grants citizens greater power to check government abuse and force even greater transparency.[6] However, as the recent and on-going battle for greater transparency in regards to national security intelligence and at the United States' Foreign Intelligence Surveillance Court (FISC) demonstrates, most government records

---

[1] *See* Craig Forcese & Aaron Freeman, The Laws of Government: The Legal Foundations of Canadian Democracy 481-84 (2005).

[2] *Id.*

[3] *Id.*

[4] *See* Steve Mann, Jason Nolan & Barry Wellman, *Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments*, 1 SURVEILLANCE & SOC'Y 331 (2003), *available at* http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3344/3306; Jean-Gabriel Ganascia, *The Generalized Sousveillance Society*, 49 SOC. SCI. INFO. 489 (2011).

[5] Jamais Cascio, *The Rise of the Participatory Panopticon*, WORLD CHANGING, (May 4, 2005), http://www.worldchanging.com/archives/002651.html; Mark A. M. Kramer, Erika Reponen & Marianna Obrist, *MobiMundi: Exploring the Impact of User-Generated Mobile Content–The Participatory Panopticon*, Proceedings of the 10th International Conference on Human Computer Interaction with Mobile Devices and Services (MobileHCI '08), at 575-577 (2008).

[6] DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? (1998); Kevin D. Haggarty & Richard V. Ericson, *The*

related to mass surveillance for foreign intelligence purposes are strictly guarded, classified, and kept from the people almost *in toto*, even when all such records might not actually reveal information that could harm the county's national security interests.

Edward Snowden's decision to leak classified intelligence documents to the press in 2013 certainly reinvigorated national and international critique of large-scale surveillance programs, but the controversies are not really all that new. Cross-border intelligence sharing between the global "Five-Eyes" countries (the USA, UK, Canada, Australia, and New Zealand) has been acknowledged for years, despite the National Security Agency (NSA) only recently declassifying certain historical documents about the UKUSA agreement and its early predecessors in the aftermath of the Second World War.[7] These collaborative efforts encompass a truly global infrastructure, and they are undoubtedly highly effective at neutralizing a variety of national security threats. They also pose some difficult questions for democratic governance and individual liberty.

For example, cross-border information sharing without strict and clearly worded regulations may potentially allow governments to evade domestic restrictions on directly collecting intelligence information about their own citizens. In addition, the string of revelations following Snowden's initial disclosures reinforce the fact that governments are maintaining arguably outdated legal standards about the differences between metadata–or information about information–and the substantive contents of communications. These legal allowances for substantial metadata surveillance pose serious risks to individual privacy and, given the modern reality that information equals (or at least facilitates) power, potentially allow governments to impermissibly interfere with individual liberty and, ultimately, to arbitrarily dominate the citizenry they are supposed to represent.

This paper explores the relationship between liberty and security implicated by secret government surveillance programs, with an emphasis on the U.S. experience. It includes both doctrinal analysis of

---

New Politics of Surveillance and Visibility, THE NEW POLITICS OF SURVEILLANCE AND VISIBILITY 10 (K.D. Haggarty & R.V. Ericson eds., 2006).

[7] *See e.g.* European Parliament Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)), EUR. PARL. DOC. (A5-0264) 59 (2001), *available at* http://www.fas.org/irp/program/process/rapport_echelon_en.pdf. For information about the declassification by the NSA of the early UKUSA Agreement documents in 2010, *see* Press Release, National Security Agency, Declassified UKUSA Signals Intelligence Agreement Documents Available (June 24, 2010), *available at* http://www.nsa.gov/public_info/press_room/2010/ukusa.shtml.

case law in the United States and at the European Court of Human Rights (ECtHR) as well as theoretical analysis informed by political theory and literature within the burgeoning field of surveillance studies. Methodologically, the paper examines judicial reasoning in cases where parties have challenged secret government surveillance programs on constitutional or human rights grounds. In doing so, this paper will question how liberal and neorepublican conceptions of liberty, defined as the absence of actual interference and the possibility of arbitrary domination, respectively, can inform the way we think about the proper relationship between security and liberty in the post-9/11, post-Snowden world. This paper will also explore how needed legal protections for non-content information (metadata) can effectively aid in reducing the potential of government domination.

The argument presented in this paper leads to the conclusion that governments must allow their citizens enough access to information necessary for individual self-government. Greater protections for some types of metadata and aggregate communications data may need to be implemented to effectively reduce the risk of actual interference and arbitrary domination. To be fully non-arbitrary and non-dominating, government must also respect and provide effective institutional and legal mechanisms for their citizenry to effectuate self-government and command noninterference. Establishing liberal access rights to information about government conduct and mechanisms that ensure that citizens can effectively command noninterference are justified on the grounds that they reduce the possibility of arbitrary, and actual, interference with the right of the people to govern themselves. Such measures would also limit the institutionalization of systemic domination within political and social institutions. In an age when technology has "changed the game"[8] by removing barriers to the government's ability to access, aggregate, and utilize the personal information of the people, the law should similarly adapt and provide citizens with rights to counter the otherwise inevitable power imbalance, through greater privacy protections and/or enhanced access to government information.

II. MASS SURVEILLANCE AND NATIONAL SECURITY

Mass surveillance is not entirely new, although advances in technology continue to supplement the abilities of governments to gather greater amounts of information much more efficiently. Additionally, cross-border intelligence operations and information-

[8] ADAM D. MOORE, PRIVACY RIGHTS: MORAL AND LEGAL FOUNDATIONS 4 (2010).

sharing between domestic and foreign intelligence agencies is a long documented reality. Recent revelations that the NSA has been sharing raw, un-redacted, intelligence information (including information about American citizens) with Israel with few strings attached[9] may have surprised some, but is consistent with the historical trajectory of cross-border intelligence sharing by the NSA and its predecessors.

International signals intelligence (SIGINT) sharing owes its roots, at least in part, to a British-USA intelligence sharing arrangement, later formalized as the "BRUSA" Circuit and then the UKUSA Agreement, which began to take shape as early as 1940, when the British government requested the exchange of secret intelligence information and technical capabilities with the United States.[10] This information-sharing association is often now referred to as Echelon or "Five Eyes." In the 1940s, the two countries negotiated a number of agreements related to intelligence cooperation and information sharing, establishing a formal agreement on communications intelligence (COMINT) sharing in March of 1946.[11] In 1955 and 1956, the relationship was further formalized in an updated UKUSA agreement, which also included reference to the inclusion of Canada, Australia, and New Zealand as "UKUSA-collaborating Commonwealth countries."[12] Subsequent agreements and documents have not been declassified, however, but the continuing existence of the "Five Eyes" partnership has been confirmed.

The early UKUSA agreement was limited to COMINT matters (a subset of the larger category of SIGINT, which also includes

---

[9] Glenn Greenwald, Laura Poitras & Ewen MacAskill, *NSA Shares Raw Intelligence Including Americans' Data with Israel*, THE GUARDIAN, Sept. 11, 2013, http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.

[10] *UKUSA Agreement Release 1940-1956*, NATIONAL SECURITY AGENCY, http://www.nsa.gov/public_info/declass/ukusa.shtml (The United States National Security Agency has released declassified documents related to the early UKUSA agreement on its website); Letter from Phillip Kerr, 11th Marquess of Lothian and Ambassador to the U.S. from the U.K. to President Franklin Delano Roosevelt (July 8th, 1940), *available at* http://www.nsa.gov/public_info/_files/ukusa/early_papers_1940-1944.pdf. (The early papers, including the initial request from the British Embassy proposing the information sharing arrangement, can be found in Early Papers Concerning US-UK Agreement–1940–1944).

[11] British-U.S. Communications Intelligence Agreement and Outline, U.S.-U.K., Mar. 5, 1946, *available at* http://www.nsa.gov/public_info/_files/ukusa/agreement_outline_5mar46.pdf.

[12] U.K.–U.S. Communications Intelligence Agreement, U.S.-U.K., May 10, 1955, *available at* http://www.nsa.gov/public_info/_files/ukusa/new_ukusa_agree_10may55.pdf.

electromagnetic intelligence–or ELINT) and collateral material "for technical purposes."[13] Under the agreement, the national agencies pledged to exchange the following COMINT products: 1) collection of traffic, 2) acquisition of communications documents and equipment, 3) traffic analysis, 4) cryptanalysis, 5) decryption and translation, and 6) acquisition of information regarding communications organizations, procedures, practices and equipment.[14]

The United States and many other countries have also subsequently entered into treaties with a number of foreign states to share information and assist foreign law enforcement agencies to investigate and prosecute crime and terrorism. Generally, these agreements are called Mutual Legal Assistance Treaties (MLATs). As an example, Canada and the United States signed a Mutual Legal Assistance Treaty (the "CAN-US MLAT") in 1985 which focused on cooperation in criminal matters.[15] The CAN-US MLAT, which is similar in many regards to treaties the U.S. has negotiated with a number of other countries, provides that the two countries shall provide "mutual legal assistance in all matters relating to the investigation, prosecution and suppression of offences,"[16] including "exchanging information . . . locating or identifying persons . . . providing documents and records . . . [and] executing requests for searches and seizures."[17]

In the years between 9/11 and Edward Snowden's leaking documents to the press in 2013, national communications and foreign intelligence programs changed from a "need to know"[18] mentality to a "new culture of 'need to share.'"[19] As then Director of National

---

[13] *Id.* at para. 2.

[14] *See* U.K.–U.S. Communications Intelligence Agreement (UKUSA Agreement) at 5, U.S.-U.K., May 10, 1955*, available at* http://www.nsa.gov/public_info/_files/ukusa/new_ukusa_agree_10may55.pdf.

[15] Treaty between the Government of Canada and the Government of the United States of America on Mutual Legal Assistance in Criminal Matters, U.S.-Can., Mar. 18, 1985, 24 I.L.M. 1092 (1985), *available at* http://www.treaty-accord.gc.ca/text-texte.aspx?id=101638 [hereinafter "CAN-US MLAT"].

[16] *Id.* at art. II, para. 1.

[17] *Id.* at art. II, paras. 2(b), (c), (f), and (h).

[18] THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, 417 (2004).

[19] Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 951, 951 (2006), (citing 9/11 COMMISSION REPORT, *supra* note 18, at 417).

Intelligence Dennis Blair noted in his Preface to the 2009 National Counterintelligence Strategy, information sharing has led to greater vulnerabilities, which requires greater collaboration and coordination between intelligence agencies.[20] Based on Snowden's recent revelations and earlier reports, we know that government agencies, and particularly the NSA, have been collecting and analyzing vast quantities of telecommunications metadata as well as other online information from social media and online communications providers for quite some time. These disclosures have also led to the Director of National Intelligence (DNI) declassifying a number of surveillance-related documents and legal decisions,[21] as well as to a series of privately initiated lawsuits.[22]

III. THE (META)DATA PROBLEM

Metadata, commonly defined as "information about information" or "data about data," includes (in the context of electronic communications) information about the time, duration, and location

---

[20] Dennis C. Blair, *Preface* to OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE, THE NATIONAL COUNTERINTELLIGENCE STRATEGY OF THE UNITED STATES OF AMERICA, iii (2009), *available at* http://www.ncix.gov/publications/strategy/docs/NatlCIStrategy2009.pdf.

[21] *See, e.g.*, Press Release, Office of the Director of National Intelligence, DNI Clapper Declassifies Additional Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (Nov. 18, 2013), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/964-dni-clapper-declassifies-additional-intelligence-community-documents-regarding-collection-under-section-501-of-the-foreign-intelligence-surveillance-act-nov (documents posted to http://icontherecord.tumblr.com/tagged/declassified); Press Release, Office of the Director of National Intelligence, DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001 (Dec. 21, 2013) *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/991-dni-announces-the-declassification-of-the-exisitence-of-collection-activities-authorized-by-president-george-w-bush-shortly-after-the-attacks-of-september-11,-2001 [hereinafter Press Releases].

[22] *See, e.g.*, ACLU v. Clapper, 2013 WL 6819708 (S.D.N.Y. Dec. 27, 2013) (rejecting Fourth Amendment claims based on government telephone and metadata surveillance, but granting standing on metadata issue); Klayman v. Obama, 2013 WL 6571596 (D.D.C. Dec. 16, 2013) (finding NSA surveillance probably violates the Fourth Amendment, in suit alleging the government's PRISM program violated privacy and First Amendment rights); First Unitarian Church of Los Angeles v. NSA, First Amended Complaint, 2013 WL 5311964 (N.D. Cal. Sept. 10, 2013) (alleging constitutional violations of government's dragnet telephone surveillance activities); *In re* Electronic Privacy Information Center, 134 S.Ct. 638 (2013) (denying cert).

of a communication as well as the phone numbers or email addresses of the sending and receiving parties. It also may include information about the device used, for example, the make/model and specific device identification number. Metadata is generated whenever a person uses an electronic device (such as a computer, tablet, mobile phone, landline telephone, or even a modern automobile) or an electronic service (such as an email service, social media website, word processing program, or search engine). Often, this results in the creation of considerable amounts of information (metadata). At least with regard to telephone metadata, service providers collect and retain this information in databases that often can be traced directly to an individual person.

However, metadata is not just associated with electronic communications, it also serves to document various properties of other facts, documents, or processes. For example, automated license plate recognition systems create metadata about the locations of vehicles at certain points in time. Taking a digital photograph often creates metadata about the location the photograph was taken, the aperture, focal length, and shutter speed settings of the camera. Word processing programs such as Microsoft Word also save metadata such as the name of the author who created the document, the date of creation, the date on which the latest changes have been made, the name of the user who made the most recent changes, the total number of words and pages in a document, and the total length of time that a document has actually been edited.

A. *Metadata and Surveillance after Edward Snowden*

After Edward Snowden leaked classified NSA documents to the press in mid-2013, questions about the nature of government collection of communications metadata took a prominent place on the world stage. Snowden's first revelation was a classified court order from the secretive FISC that compelled Verizon, one of the largest U.S. telecommunications providers, to provide the U.S. government with all of its customers' telephone metadata on an ongoing basis– encompassing landline, wireless and smartphone communications.[23] Other disclosures indicate that the three major U.S. telecommunications companies were subject to similar orders[24] and

[23] Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN, June 5, 2013, *available at* http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

that NSA surveillance covered approximately 75% of all Internet traffic in the U.S., including email.[25]

In a Congressional hearing, top U.S. officials claimed that they were only collecting information about numbers of the parties to communications (the sender and receiver of phone calls) and the duration of the calls. NSA and Justice Department officials, and high-ranking Congressional representatives, also claimed that since they were not collecting the actual contents of communications (e.g. the words spoken), the surveillance did not invade anyone's reasonable expectations of privacy. The officials claimed explicitly that they were not collecting geo-location data (e.g. the geographic location of the device when the call was made or received),[26] but nothing in the FISC order limited the government from obtaining this kind of information as well. Importantly, the U.S. authorities are legally restricted from collecting the actual contents only of Americans' communications under the U.S. Constitution and of communications by non-citizens lawfully within the U.S., as the government is legally permitted to collect the contents (and metadata) of non-U.S. persons outside the U.S. without any prior judicial authorization.

In the months that followed, additional disclosures (approved and otherwise) continued to paint a broader picture of the NSA's domestic and international surveillance activities. The DNI declassified and released additional documents related to current and past surveillance programs.[27] The White House commissioned a Review Group on Intelligence and Communications Technologies to investigate the proper balance between personal security (privacy) and national, or

---

[24] Siobhan Gorman, Evan Perez, & Janet Hook, *U.S. Collects Vast Data Trove*, WALL ST. J., June 7, 2013, http://online.wsj.com/article/SB10001424127887324299104578529112289298922.html. For some historical precedent, *see also* Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

[25] Siobhan Gorman & Jennifer Valentino-DeVries, *NSA Reaches Deep Into U.S. To Spy on Net*, WALL ST. J., Aug. 21, 2013 at A1, *available at* http://online.wsj.com/article/SB10001424127887324108204579022874091732470.html.

[26] *See* Adam Serwer, *Is the NSA collecting cell phone location data?*, MSNBC, Sept. 27, 2013, http://tv.msnbc.com/2013/09/27/is-the-nsa-collecting-cell-phone-location-data/; *see also* Paul Lewis & Dan Roberts, *US Intelligence Chiefs Urge Congress to Preserve Surveillance Programs*, THE GUARDIAN, Sept. 26, 2013, http://www.theguardian.com/world/2013/sep/26/nsa-surveillance-senate-committee.

[27] *See* Press Releases, *supra*, note 21.

homeland, security[28] and Federal Courts have now handed down conflicting decisions about whether the NSA surveillance programs disclosed by Snowden violate the Fourth Amendment rights of American citizens.[29]

These recent disclosures of formerly classified decisions provide a glimpse into the rationale the FISC has used to authorize government metadata surveillance in the past. In a decision from the FISC,[30] likely rendered in July 2004,[31] Judge Kollar-Kotelly upheld the constitutionality of a prior bulk Internet metadata collection program that had been suspended for a period of months due to concerns about its legitimacy. This decision also marked the point when legal authorization for bulk Internet metadata surveillance transitioned from the President's Surveillance Program, spurred by President Bush's October 4, 2001 authorization memorandum, to FISC jurisdiction.[32] The prior program had been instituted by the NSA after government lawyers concluded the NSA did not "acquire" communications during bulk collection, but only after specific communications were "selected" using "selectors that met certain criteria."[33] In her decision, Judge Kollar-Kotelly recognizes that bulk metadata collection imposes a "much broader type of collection than other pen register/trap and trace applications" than the courts had grappled with before.[34] However, she ultimately concluded that the bulk collection at issue was consistent with the Foreign Intelligence

---

[28] *See* The President's Review Group on Intelligence and Communications Technologies, Report and Recommendations: Liberty and Security in a Changing World 1 (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[29] *Compare* ACLU v. Clapper, 2013 WL 6819708 (S.D.N.Y. 2013) (no violation), *with* Klayman v. Obama, 2013 WL 6571596 (D.D.C. 2013) (probable violation).

[30] [case name redacted], No. PR/TT [redacted], slip op. at 80 (FISA Ct.), *available at* http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf [hereinafter Kollar-Kotelly Opinion].

[31] The date on the Kollar-Kotelly Opinion is redacted, but probable references to the decision can be found in the 2009 Working Draft from the Office of the Inspector General to the NSA and CIA leaked by Edward Snowden in June 2013. *See* OFFICE OF INSPECTOR GENERAL, NATIONAL SECURITY AGENCY, WORKING DRAFT 39, *available at* http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection#document/ [hereinafter IG WORKING DRAFT].

[32] IG WORKING DRAFT, *supra* note 31, at 39.

[33] *Id.* at 38.

[34] Kollar-Kotelly Opinion, *supra* note 30, at 2.

Surveillance Act (FISA)[35] and the First and Fourth amendments to the Constitution, with some modifications (e.g. NSA analysts could only conduct approved queries).[36]

In another FISC decision, a few years later, Judge Bates re-authorized the bulk collection of metadata about Internet communications.[37] In his decision, Judge Bates notes that the NSA acknowledged that it had exceeded the scope of its authorization under earlier orders for a matter of years.[38] Despite that acknowledgement, the government also sought authorization from the FISC to query and search through the previously collected data, whether or not it was acquired lawfully in the first place.[39] In response to FISC inquiries about past over-collection, some of the NSA's initial assurances to the court also "turned out to be untrue."[40] However, because the government "asserted that it has a strong national security interest in accessing and using the overcollected information"[41] and "high-level officials" in the Department of Justice and NSA personally promised the FISC that they would "closely monitor" future collection, Judge Bates allowed the NSA to use and query the information collected unlawfully and approved future collection.[42] In that unfortunate (for oversight and transparency) turn, Judge Bates based much of the oversight of the program on the "good faith" of the "responsible executive branch officials"[43] who had made personal assurances to the court. In a subsequent FISC decision, Judge Walton noted that the government had disclosed a number of additional compliance problems and continued to inadequately conform to the requirements of FISC orders authorizing and regulating intelligence collection under both the Internet surveillance

---

35 Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801-1811 (2002); 18 U.S.C. §§ 2511, 2518-19 (2002)).

36 Kollar-Kotelly Opinion, *supra* note 30, at 2.

37 [case name redacted], No. PR/TT [redacted], slip op. at 2 (FISA Ct.), *available at* http://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf [hereinafter Bates Opinion].

38 *Id.* at 2-3.

39 *Id.* at 1-2.

40 *Id.* at 11.

41 *Id.* at 115-16.

42 *Id.* at 116.

43 *Id.*

program and a similar metadata surveillance program targeting telephone communications.[44]

B. *Problems with Binary Fourth Amendment Theory*

Much of the metadata surveillance conducted by the NSA, including the harvesting of telephone records of U.S. citizens, is permitted, legally, based on Supreme Court decisions about the appropriate expectation of privacy that individuals may hold in "non-content" (metadata) information.[45] These cases held that citizens cannot claim privacy interests, *vis-à-vis* the government, in records turned over to a third-party (bank records)[46] or in the numbers dialed from a telephone[47] (although, as indicated in Judge Kollar-Kotelly's opinion, bulk collection is quite a bit broader than traditional pen register or trap and trace orders).[48] As a consequence, legal definitions of privacy (at least in the Fourth Amendment search context) have often been crafted to force conclusions about potential privacy violations based on binary distinctions: either a form of investigation or information gathering by government agents constitutes a search or it does not.[49] The binary nature of this analysis itself is not inherently

---

[44] *In Re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [redacted], no. BR 09-06, slip op. at 2 (FISA Ct.), *available at* http://www.dni.gov/files/documents/1118/CLEANED101.%20Order%20and%20Supplemental%20Order%20%286-22-09%29-sealed.pdf [hereinafter Walton Opinion].

[45] *See* Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976). For a recent FISC decision reaffirming this point, *see In Re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [redacted], No. BR 13-109, slip op. at 2 (FISA Ct.) (as amended and released on Sept. 17, 2013) *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf [hereinafter the Eagan Opinion]; *see also* United States v. D'Andrea, 497 F. Supp. 2d 117, 120 (D. Mass., 2007); Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (holding that a user loses any expectation of privacy in personal subscription information when it is conveyed to a system operator); United States v. Cox, 190 F. Supp. 2d 330, 332 (N.D.N.Y. 2002) ("[C]riminal defendants have no Fourth Amendment privacy interest in subscriber information given to an internet service provider."); Bryce Clayton Newell, *Rethinking Reasonable Expectations of Privacy in Online Social Networks*, 17 RICH. J.L. & TECH. 12, 32 (2011), *available at* http://jolt.richmond.edu/v17i4/article12.pdf.

[46] United States v. Miller, 425 U.S. 435 (1976).

[47] Smith v. Maryland, 442 U.S. 735 (1979).

[48] *See* Kollar-Kotelly Opinion, *supra* note 30.

[49] *See* Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).

problematic–in fact it may be highly desirable to draw clear lines governing law enforcement action. However, certain strict application of binary tests developed in past cases, without reconsideration of the rapid developments in information technologies and the scope of possible government intrusion into private life through massive metadata acquisition programs, may improperly restrict Fourth Amendment protections of personal privacy.

A recent FISC decision[50] upholding the constitutionality of the FBI/NSA telephone metadata surveillance program authored by Judge Claire Eagan and released on September 17, 2013, failed to take account of potentially important dicta in Supreme Court's decision in *United States v. Jones*.[51] In that case, the Justices held that the warrantless application of a GPS tracking device to a suspect's automobile violated the suspect's Fourth Amendment rights. In two concurring opinions signed by five justices, Justices Sotomayor and Alito separately argued that aggregated geo-locational metadata ought to raise a reasonable expectation of privacy.[52]

Because of the concurring opinions in *Jones*, which signal the possibility that a majority of the Justices might be open to revisiting Fourth Amendment theory in light of modern technologically-aided police practices,[53] it may be an opportune time to argue for a normative approach to privacy in Fourth Amendment jurisprudence that is more sensitive to context (not bound by purely binary distinctions) and the increasingly revealing capacity of metadata surveillance, especially when such information is collected, stored, and mined in the aggregate.

IV. SECRET SURVEILLANCE CASE LAW: THE U.S. AND EUROPE

Courts around the world have grappled with the legal issues implicated by secret government surveillance programs for a number of years. The two succeeding sections provide an overview of some of the important cases in the United States and at the ECtHR.

---

[50] Eagan Opinion, *supra* note 45.

[51] 132 S. Ct. 945 (2012).

[52] *Id.* at 954 (Sotomayor, J. concurring); *Id.* at 958 (Alito, J. concurring).

[53] Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320 (2012) ("A close reading of *Maynard/Jones* suggests that five Justices are ready to embrace the new mosaic approach to the Fourth Amendment: Justices Ginsburg, Breyer, Alito, Kagan, and Sotomayor.").

A. *The European Court of Human Rights*

The ECtHR has a long history of decisions questioning whether secret government surveillance is conducted consistently with the provisions of Article 8 of the European Convention on Human Rights (the "Convention").[54] The Convention acts (along with individual state constitutions) as one European corollary to the U.S. Constitution, and functions as a basic limit on government authority to conduct domestic (and international) surveillance, albeit at a supranational level.

The first relevant ECtHR case is *Klass and Others v. Germany*[55] from 1978. In that case, Klass and four other applicants challenged provisions of a German surveillance statute on two primary grounds; first, that the act did not require the government to notify targets of surveillance after the surveillance had concluded and, second, that the act excluded remedies before regular domestic courts.[56] Ultimately, the ECtHR found no violation of the applicants' Article 8 rights, but the court outlined the relevant test to determine when secret surveillance powers might violate a person's basic human rights. This test has been largely adopted in recent cases, with some modifications (including more restrictive requirements when determining whether conduct is "in accordance with law").

Article 8 of the Convention states (in relevant part):

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in

---

[54] The primary cases cited in ECtHR jurisprudence are Klass v. Germany, App. No. 5029/71, 2 Eur. H.R. Rep. 214 (ser. A) (1978) [hereinafter *Klass*]; Malone v. United Kingdom, App. No. 8691/79, 7 Eur. H.R. Rep 14 (1984) [hereinafter *Malone*]; Weber v. Germany, App. No. 54934/00, 2006-XI Eur. Ct. H.R. 1173 [hereinafter *Weber*]; Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, App. No. 62540/00, 2007 Eur. Ct. H.R. 533 [hereinafter *Ekimdzhiev*]; Liberty v. United Kingdom, App. No. 58243/0, 2008 Eur. Ct. H.R. 568 [hereinafter *Liberty*]; and Iordachi v. Moldova, App. No. 25198/02, 2009 Eur. Ct. H.R. 256 [hereinafter *Iordachi*].

[55] *Klass*, *supra*, note 54.

[56] *Id.* at paras. 10, 26.

> accordance with the law and is necessary in a democratic society....[57]

The applicants in *Klass* were lawyers who regularly represented individuals they suspected of being under surveillance. These attorneys concluded that their own communications might also have been intercepted, and initiated claims to challenge the surveillance as a violation of their Article 8 rights. The European Commission on Human Rights (the "Commission") declared the application admissible to the ECtHR, essentially holding that the applicants had standing. Despite the fact that only "victims" of alleged violations of the Convention could bring cases before the ECtHR, the Commission found that,

> As it is the particularity of this case that persons subject to secret supervision by the authorities are not always subsequently informed of such measures taken against them, it is impossible for the applicants to show that any of their rights have been interfered with. In these circumstances the applicants must be considered to be entitled to lodge an application even if they cannot show that they are victims.[58]

In its subsequent decision, the ECtHR agreed, holding that, "an individual may, under certain conditions, claim to be the victim of a violation occasioned by the mere existence of secret measures or of legislation permitting secret measures, without having to allege that such measures were in fact applied to him."[59]

The ECtHR noted that to hold otherwise might reduce Article 8 to a "nullity," since a state could potentially violate a person's rights in secret, without any risk that a person could bring a claim for relief.[60] Thus, the ECtHR confirmed the Commission's decision on the admissibility of the application. Having determined the application

---

[57] European Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Apr. 11, 1950, 213 U.N.T.S. 221 (as amended), *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm (entered into force Sept. 3, 1953) [hereinafter ECHR].

[58] *Klass*, *supra* note 54, at para. 27; *cf.* Clapper v. Amnesty International USA, 133 S.Ct. 1138 (2013).

[59] *Klass*, *supra* note 54, at para. 34.

[60] *Id.* at para. 36.

admissible, the court addressed the threshold Article 8 question: whether the activity complained of constituted an interference with the applicant's "right to respect for his private and family life, his home and his correspondence."[61] The court found that "the mere existence of the legislation" constituted a "menace" of surveillance which, "necessarily strikes at freedom of communication between users of the postal and telecommunication services and thereby constitutes an 'interference by a public authority' with the exercise of the applicants' right to respect for private and family life and for correspondence."[62]

The court then addressed whether the surveillance regime was otherwise justified. First, the court found that, since the surveillance at issue had its basis in an Act of the German Parliament, it was done in "accordance with the law." Second, the court also held, simply, that the aim of the surveillance was for legitimate purposes, namely, to protect national security and for the prevention of disorder or crime.[63] The more difficult question, according to the court, was: "whether the means provided under the impugned legislation for the achievement of the above-mentioned aim remain in all respects within the bounds of what is necessary in a democratic society."[64]

The court conceded that in extraordinary circumstances, legislation that provides for secret surveillance of physical or electronic communication can be "necessary in a democratic society."[65] In coming to this conclusion, the court took judicial notice of the facts that surveillance technology was rapidly advancing and that European states did find themselves threatened by sophisticated terrorists.[66] As such, domestic legislatures should enjoy some, but not unlimited, discretion in outlining government surveillance powers.[67] However, because such laws pose a danger of "undermining or even destroying democracy on the ground of defending it," legislatures may not, simply "adopt whatever measures they deem appropriate" in their

---

[61] ECHR, *supra* note 57, at art. 8.

[62] Klass, *supra* note 54, at para. 41.

[63] *Id.* at para. 46.

[64] *Id.*

[65] *Id.* at para. 48.

[66] *Id.*

[67] *Id.* at para. 49.

"struggle against espionage and terrorism."[68] Getting to the heart of whether such surveillance is necessary in a democratic society, the court stated, "whatever system of surveillance is adopted, there [must] exist adequate and effective guarantees against abuse."[69]

The court concluded that the German law did not violate the applicants' Article 8 rights because the law limited the ability of the government to conduct surveillance, "to cases in which there are factual indications for suspecting a person of planning, committing or having committed certain serious criminal acts," and that, "[c]onsequently, so-called exploratory or general surveillance is not permitted by the contested legislation."[70] This test has been largely adopted in subsequent ECtHR decisions, with some modifications (including more restrictive requirements when determining whether conduct is "in accordance with law") developing in a few important cases. The analysis below provides an overview of the court's reasoning and relevant case law, as announced in its most prominent subsequent cases.

Because of the secret nature of the surveillance at issue, the ECtHR has generally allowed applicants' standing, even without having to allege facts that would support a finding that the secret surveillance was actually applied to them.[71] In recent cases, the ECtHR continues to adhere to the finding announced in *Klass* that the mere existence of legislation allowing secret surveillance constitutes an interference with a person's Article 8 rights[72]–specifically "private life" and "correspondence."[73] In *Malone v. the United Kingdom*,[74] in 1984, the ECtHR reaffirmed this position, holding that because telephone conversations fell within the scope of "private life" and "communications," the existence of legislation that allowed the interception of telephone conversations amounted to an interference

---

[68] *Id.*

[69] *Id.* at para. 50.

[70] *Id.* at para. 51.

[71] This was initially determined in *Klass*, *supra* note 54, but has been favorably cited and applied in recent cases as well; *see, e.g.*, *Iordachi*, *supra* note 54.

[72] The primary cases cited in ECtHR jurisprudence are *Klass*, *supra* note 54; *Malone*, *supra* note 54, at para. 64; *Weber*, *supra* note 54, at paras. 77-79; *Ekimdzhiev*, *supra* note 54, at para. 69; *Liberty*, *supra* note 54, at para. 57; and *Iordachi*, *supra* note 54, at para. 34. A number of other cases also recite this proposition.

[73] *Liberty*, *supra* note 54, at para. 56; *Weber*, *supra* note 54, at para. 77.

[74] *Malone*, *supra* note 54.

with the applicant's rights.[75] This extends to general programs of surveillance as well as targeted eavesdropping on private conversations.[76] Because of the essentially settled nature of this finding, most of the interesting judicial reasoning happens in answering the subsequent questions.

Initially, the requirement that an act of interference must be in accordance with the law was also easy to overcome. In *Klass*, the ECtHR held that since the surveillance at issue, the alleged interception of the applicants' telephone calls, had its basis in an Act of the German Parliament that specifically authorized such measures, it was done in accordance with the law.[77] However, in subsequent cases, the ECtHR has added additional tests to determine the answer to this question. By 1984, the *Malone* court recognized that this requirement also demanded more than just compliance with domestic law. Quoting from intervening judgments of the Court, the *Malone* court stated,

> Firstly, the law must be adequately accessible: the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a given case. Secondly, a norm cannot be regarded as "law" unless it is formulated with sufficient precision to enable the citizen to regulate his conduct: he must be able—if need be with appropriate advice—to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail.[78]

These requirements of accessibility, foreseeability and compatibility with the rule of law were announced in the *Malone* case, and have been reaffirmed in subsequent surveillance cases. At present, for an interference to be conducted in accordance with the law, as the Convention requires, the ECtHR must be satisfied that, as a threshold matter, the surveillance has some basis in domestic law. If it does, the Court then determines whether the "quality of the law" is

---

[75] *Id.* at para. 64.

[76] *Liberty*, *supra* note 54, at para. 63.

[77] *Klass*, *supra* note 54, at para. 43.

[78] *Malone*, *supra* note 54, at para. 66 (quoting Sunday Times v. United Kingdom, 30 Eur. Ct. H.R (ser. A) para. 49 (1979)); Silver v. United Kingdom, App. No. 5947/72, 1983 Eur. Ct. H.R. 5, paras. 87-88.

sufficient; that is, 1) the enabling law must be "accessible to the person concerned," 2) the person must be able to foresee the consequences of the law for him- or herself,[79] and 3) the law itself must be compatible with the rule of law.[80]

In *Weber and Saravia v. Germany*,[81] the applicants claimed violations under the same German eavesdropping law that was at issue in *Klass*. Rather than taking issue with targeted interception of telecommunications of specific individuals, however, the applicants in the *Weber* case claimed that their Article 8 rights had been violated by a broader intelligence practice of "strategic monitoring" of telecommunications and the subsequent uses of such information (including information-sharing with other agencies).[82] In that case, the ECtHR found that the domestic courts had determined the surveillance at issue was covered by domestic law, and that, "the Court cannot question the national courts' interpretation except in the event of flagrant non-observance of, or arbitrariness in the application of, the domestic legislation in question."[83] In a number of other cases, the parties and the court simply accept that the surveillance at issue has the requisite basis upon a showing by the government that some relevant law exists.[84]

The "accessibility" and "foreseeability" requirements are often intertwined in the ECtHR's analysis, although sometimes the issue of accessibility is separated from the foreseeability inquiry, and is not given as much direct consideration by the Court.[85] In *Liberty v. the United Kingdom*, the applicant charity organization alleged that the UK Ministry of Defence operated a facility that was capable of intercepting 10,000 simultaneous telephone channels operating between Dublin to London and from London to the European

---

[79] *Weber*, *supra* note 54, paras. 93-95 (for the most recent detailed elaboration of this requirement); *Liberty*, *supra* note 54, at para. 59-63; *Ekimzheiv*, *supra* note 54, at paras. 74-77.

[80] *Weber*, *supra* note 54, at para. 84, (citing Kruslin v. France, Eur. Ct. H.R. 10, at para. 27 (1990)); *Ekimdzhiev*, *supra* note 54, at para. 71; *Liberty*, *supra* note 54, at para. 59; *Iordachi*, *supra* note 54, at para. 37.

[81] *Weber*, *supra* note 54.

[82] *Id.* at para. 4.

[83] *Id.* at para. 90.

[84] *See e.g. Ekimdzhiev*, *supra* note 54, at para. 72; *Iordachi*, *supra* note 54, at para. 38; *Liberty*, *supra* note 54, at para. 60.

[85] *See Ekimdzhiev*, *supra* note 54, at para. 73; *Weber*, *supra* note 54, at para. 92.

Continent, as well as a certain amount of radio-based telephone, facsimile, and email communications carried between two British Telecom stations.[86] The government refused to confirm or deny the specific allegations, but agreed, for purposes of the litigation, that the applicants were of the category of legal persons who could be subject to having their communications intercepted by the government under its intelligence gathering programs.[87]

The government further claimed that revealing additional information about the specific arrangements authorized by the Secretary of State in relation to any warrants issued would compromise national security secrets.[88] They also refused to disclose the manuals and instructions which detailed the safeguards and arrangements put in place to govern the use of the program.[89] In their defense, the government stated that "the detailed arrangements were the subject of independent review by the successive Commissioners, who reported that they operated as robust safeguards for individuals' rights."[90]

Liberty argued that the secret nature of the Secretary's "arrangements" under the Interception of Communications Act rendered these procedures and safeguards inaccessible to the public and made it impossible for the public to foresee how and in what circumstances the government could intercept their communications.[91] The ECtHR agreed with the government's contentions that all the elements of the accessibility and foreseeability requirements did not need to be specified in primary legislation (for example, they could be specified in administrative orders and other soft law sources), but that secondary sources could satisfy this requirement "only to 'the admittedly limited extent to which those concerned were made sufficiently aware of their contents.'"92

However, the ECtHR held that the government had violated the applicants' Article 8 rights in that case. The court came to this conclusion for a few reasons. First, the accessible law did not place

---

[86] *Liberty*, *supra* note 54, at para. 5.

[87] *Id.* at para. 47.

[88] *Id.* at para. 48.

[89] *Id.*

[90] *Id.*

[91] *Id.* at para. 60.

[92] *Liberty*, *supra* note 54, at para. 61 (quoting *Malone*, *supra* note 54).

any restrictions on the type of external (non-UK) communications that could be included in a warrant, a fact that the court found indicative of "virtually unfettered" executive discretion.[93] Second, the Act granted wide discretion to the authorities to determine which of the collected communications to actually review substantively. The Secretary of State could issue certificates describing material to be examined, using broad limiting terms and reasons such as "national security" to authorize review of the contents of communications.[94] These certificates could be applied to all communications except those "emanating from a particular address in the United Kingdom," unless the Secretary determined such interception was necessary to prevent or detect acts of terrorism.[95] The Act also required the Secretary to "'make such arrangements as he consider[ed] necessary' to ensure that material not covered by the certificate was not examined and that material that was certified as requiring examination was disclosed and reproduced only to the extent necessary."[96]

Importantly, details of these arrangements were secret and not made accessible to the public.97 A Commissioner did make annual reports stating that the Secretary's arrangements were in accordance with the law, but the ECtHR held that, while these reports were helpful, did not make the details of the scheme any more clear or accessible to the public, since the Commissioner was not allowed to reveal details about the arrangements in his public reports.98 Indeed, the court stated that, "the procedures to be followed for examining, using and storing intercepted material, inter alia, should be set out in a form which is open to public scrutiny and knowledge."[99]

The ECtHR dismissed the government's claims that revealing such information publicly would damage the efficacy of the government's intelligence operations because, as indicated in its earlier decision in Weber, the German government had included such guidelines and

---

[93] *Id.* at para. 64.

[94] *Id.* at para. 65

[95] *Id.*

[96] *Id.* at para. 66.

[97] *Id.*

[98] *Liberty*, *supra* note 54, at para. 67.

[99] *Id.*

restrictions in its primary (and publicly accessible) legislation itself.[100]

In conclusion, the court held that the domestic law did not "provide adequate protection against abuse of power" because of its broad scope and the "very wide discretion conferred on the State to intercept and examine external communications."[101] The court found it particularly important that the government did not make its procedures for "examin[ing], sharing, storing and destroying intercepted material" accessible to the public.[102]

In Weber, the court also laid out these requirements in some detail. In that case, the Court stated that,

> [W]here a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated. . . . Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.[103]

In the case of *Iordachi and Others v. Moldova*,[104] the Court also found a violation of Article 8. In that case, the court found that the Moldovan law at issue lacked adequate clarity and detail because 1) there was no judicial control over the granting of applications for

---

[100] *Id.* at para. 68.

[101] *Id.* at para. 69.

[102] *Id.* at para. 69.

[103] *Weber*, *supra* note 54, at paras 93-94 (citation omitted) (this language was also cited approvingly in *Liberty*, *supra* note 51).

[104] *Iordachi*, *supra* note 54.

interceptions, 2) the law was very open-ended in regards to the persons potentially within its reach, and 3) the requirements for granting warrants were imprecise.[105] Even after the Moldovan government modified its law to provide for judicial approval of warrants and the definition of a general class of crimes subject to justify interception, the Court felt it had not gone far enough.[106] Additionally, the Court stated that the legislation lacked precise details about how the government should screen gathered intelligence for useful information, preserve its integrity and confidentiality, and provide for its destruction.[107] Interestingly, the ECtHR also stated that the Moldovan secret surveillance system appeared "overused" since the courts approved "virtually all" of the prosecutor's requests for warrants. The court also noted that the numbers of issued warrants each year over a three-year period (2,300, 1,900, and 2,500, respectively) was indicative of "inadequacy" in the "safeguards contained in the law."[108]

Additionally, under Article 8 jurisprudence, the law at issue must itself be compatible with the broader notion of the rule of law. In *Weber*, the ECtHR found that the German law in question did contain adequate safeguards against arbitrary interference.[109] In the *Ekimdzhiev*[110] case, the court found that a Bulgarian law provided sufficient safeguards, at the authorization stage, so that if it were "strictly adhered to" only specifically delineated forms of communications would be intercepted.[111] However, because the law did not provide for any independent review of the intelligence agency's implementation of these measures after the initial authorization stage, it failed to satisfy the requirement that it provide adequate guarantees against the risk of abuse.[112]

The ECtHR also found that, although the lack of provisions requiring notification to a person that their communications had been

---

[105] *Id.* at para. 41.

[106] *Id.* at paras. 43-44.

[107] *Id.* at para. 48.

[108] *Id.* at para. 52.

[109] *Weber*, *supra* note 54, at para. 101.

[110] Ekimdzhiev, supra note 54.

[111] *Id.* at para. 84.

[112] *Id.* at para. 93.

intercepted was not itself unreasonable, a blanket classification of information, in perpetuity, creates the untenable situation where,

> [U]nless they are subsequently prosecuted on the basis of the material gathered through covert surveillance, or unless there has been a leak of information, the persons concerned cannot learn whether they have ever been monitored and are accordingly unable to seek redress for unlawful interferences with their Article 8 rights.[113]

Finally, if a form of interference (e.g. surveillance) passes all the prior tests (meaning it is otherwise in "accordance with law"), it must still be "necessary in a democratic society" to achieve one or more legitimate aims spelled out in the Convention. In essence, this inquiry requires a finding of proportionality, and authorities maintain a "fairly wide margin" of discretion, but such discretion is not unlimited.[114] Specifically, there must be adequate and effective guarantees to prevent abuse and, after a finding of proportionality (as the first step of this analysis), the court undertakes a holistic overall assessment (for safeguards against abuse), based on: all the facts of the case, the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law.[115]

In *Weber*, again analyzing the same German law that was at issue in *Klass* (as amended over the intervening years in subsequent cases), the Court's conclusion was not changed by the fact that in *Weber*, the applicants were complaining about broader strategic surveillance programs than those at issue in *Klass*. In *Weber*, the German government justified their continued surveillance programs on the basis that they were necessary to protect against international terrorism, specifically from threats from groups like Al-Qaida.[116] Only ten percent of telecommunications were potentially monitored, and the monitoring was limited to a limited number of specified countries.[117] The law also limited the ability of the government to monitor the telecommunications of ex-patriot Germans living abroad

---

[113] *Id.* at para. 91.

[114] *Weber*, *supra* note 54, at para. 106.

[115] *Id.*

[116] *Id.* at para. 109.

[117] *Id.* at para. 110.

and the government could not request identifying information about persons unless their communications included certain catchwords.

On the other hand, the applicants complained that the law was overbroad and that no real geographic restrictions existed, that identification could occur more easily than the government admitted, and movements of persons using cellular phones could be tracked.[118] However, despite amendments that had broadened the scope of permissible surveillance under the law, the Court found that the law continued to meet the requirements imposed by ECtHR case law because many of the restrictive limitations on authorization, implementation, and termination of surveillance continued to provide "considerable safeguards against abuse."[119] Similarly, the Court found that additional safeguards in the law rendered additional uses, transmissions, destruction, and sharing of collected information justified under the Convention.[120]

B. *The United States*

Mass communications surveillance by the U.S. Federal Government's intelligence and law enforcement agencies has been occurring for decades. Details about the BRUSA Circuit and the early UKUSA Agreement were classified until 2010 when the NSA finally declassified and revealed the early UKUSA documents[121] pursuant to an Executive Order signed by Bill Clinton fifteen years earlier.[122] In 1978, Congress enacted the Foreign Intelligence Surveillance Act (FISA) to check and balance electronic government surveillance and individual rights to privacy under the Fourth Amendment to the U.S. Constitution.[123] FISA allows the government to intercept

---

[118] *Id.* at para. 111.

[119] *Weber*, *supra* note 54, at paras. 116-18.

[120] *Id.* at paras. 128-129.

[121] *See UKUSA Agreement Release 1940-1956*, *supra* note 10; Letter from Phillip Kerr, 11th Marquess of Lothian and Ambassador to the U.S. from the U.K. to President Franklin Delano Roosevelt, *supra* note 10.

[122] Exec. Order No. 12,958, 60 Fed. Reg. 19,825 (Apr. 17, 1995), *available at* http://www.fas.org/sgp/clinton/eo12958.pdf.

[123] Diane Carraway Piette & Jesslyn Radack, *Piercing the Historical Mists: The People and Events behind the Passage of FISA and the Creation of the Wall*, 17 STAN. L. & POL'Y REV. 437, 438-439 (2006) (FISA was enacted after the Supreme Court's 1972 decision in United States v. United States Dist. Court for Eastern Dist. of Mich., 407 U.S. 297 (1972) [hereinafter "*Keith*"], in which the Court suggested that the Constitutional framework

communications involving foreign powers or "agents of foreign powers," and to maintain secrecy about whose correspondence the government has intercepted. FISA established two courts, FISC and the Foreign Intelligence Surveillance Court of Review (FISCR), drawing upon Federal judges from Article III courts to administer secret, non-adversarial, proceedings initiated by government agencies to approve government requests to collect information under FISA. Notably, court proceedings and opinions are generally secret and not available for public scrutiny. Indeed, during the first 24 years of its existence, from its inception until 2002, the FISC only ever publicly released one single opinion (which did not relate to electronic surveillance) and, it turned out, had never rejected a government application to conduct surveillance.[124]

In 2002, the FISC, acting *en banc*, publicly released an opinion signed by all seven judges that refused to allow the government to use the USA PATRIOT Act to enable closer collaboration by intelligence agents and criminal prosecutors to prosecute crimes uncovered through foreign communications intelligence surveillance.[125] Six months later, the FISCR sharply overruled the FISC opinion, holding that the FISC had "not only misinterpreted and misapplied minimization procedures it was entitled to impose. . . [it] may well have exceeded the constitutional bounds that restrict an Article III court."[126] The FISCR also stated that maintaining a divide between criminal and intelligence investigations that walled off certain investigatory and prosecutorial collaboration "was never required and was never intended by Congress."[127] In the intervening years, a number of lawsuits have emerged challenging government powers under FISA and its amending legislation, including the Foreign

---

applicable to national security cases might be different than in cases dealing with the "surveillance of 'ordinary crime."). Clapper v. Amnesty Int'l USA, 133 S.Ct. 1138, 1143 (quoting *Keith*, at 322-23).

[124] Piette and Radack, *supra* note 123, at 439; *In re* Application of United States for an Order Authorizing the Physical Search of Nonresidential Premises and Personal Property, No. 81-[Redacted] (FISA Ct. 1981) (reprinted in S. Rep. No. 97-280), *available at* http://www.intelligence.senate.gov/pdfs97th/97280.pdf (the first publicly released opinion, finding the FISC did not have statutory authority to approve warrants for physical searches).

[125] Piette and Radack, *supra* note 123, at 439.

[126] *In re* Sealed Case No. 02-001, 310 F.3d 717, 731 (FISA Ct. Rev. 2002).

[127] Neil A. Lewis, *Court Overturns Limits on Wiretaps to Combat Terror,* N.Y. TIMES, Nov. 19, 2002; Piette & Radack, *supra* note 123, at 440.

Intelligence Surveillance Amendments Act (FISA Amendments Act)[128] and the USA PATRIOT Act.[129] The purpose of this section is not necessarily to document each and every case, but rather to explore the judicial reasoning that pervades these decisions.

In February 2013, the United States Supreme Court decided *Clapper v. Amnesty International USA*,[130] which stands in fairly sharp contrast to the line of ECtHR cases beginning with *Klass*, as discussed above. In *Clapper*, the Court rejected a challenge to the constitutionality of FISA mounted by a number of attorneys and a variety of other human rights, legal, media, and labor organizations. In that case, the plaintiffs sued the United States government, claiming that surveillance authorized under section 1881a (otherwise known as section 702; enacted in 2008 by the FISA Amendments Act) violated their Constitutional rights. The organizations claimed, as did the attorneys in *Klass*, that, because of their regular communications with overseas persons, there was an "objectively reasonable likelihood that their communications will be acquired under section 1881a at some point in the future," and that the threat of this this acquisition had caused them to take costly preventative measures aimed at preserving the confidentiality of their communications.[131]

Despite the fact that, due to the law's secrecy requirements, the government is the only entity that knows which communications have been intercepted, the Court held that third-parties like Amnesty International do not have standing to challenge the Act because they cannot show that they have been harmed[132] (precisely because they don't have access to information about the government's surveillance activities). Unlike at the ECtHR, the Supreme Court held that the mere existence of secret surveillance did not grant standing, effectively blocking any challenge to secret programs absent some form of prior disclosure.

Enter Edward Snowden.

---

[128] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-126, 122 Stat. 2436 (2008).

[129] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered sections of the U.S.C.) [hereinafter PATRIOT Act].

[130] Clapper v. Amnesty International USA, 133 S.Ct. 1138 (2013).

[131] *Id.* at 1143.

[132] *Id.* at 1155.

In May 2013, Snowden leaked a secret FISC order[133] (the Verizon Order) to Guardian journalist Glenn Greenwald (which was published on June 5). In that order, the FISC directed Verizon, one of the largest telecommunications providers in the United States, to turn over phone call metadata on millions of Americas to the NSA on an on-going and daily basis.[134] Justice Claire Eagan's decision, released September 17, 2013, upheld a subsequent order requiring similar, continued compliance by an unnamed telecommunications provider.[135] Following the Guardian's publication of the Verizon Order, the American Civil Liberties Union (ACLU) and New York Civil Liberties Union (NYCLU) filed a lawsuit against the NSA.[136] Both the ACLU and NYCLU claimed standing in their complaint because they were actually Verizon customers during the dates covered by the FISC order.[137]

In 2006, the Electronic Frontier Foundation (EFF) sued AT&T for violating its customers' privacy by collaborating with the NSA to conduct electronic surveillance of its customers.[138] In response to this case, and dozens of other lawsuits fueled by news reports of the government's warrantless surveillance program, Congress enacted section 802 of the FISA Amendments Act to grant these corporations retroactive immunity.[139] Subsequently, in 2008, EFF filed suit against the NSA and various other federal entities in *Jewel v. NSA*[140] claiming that the same warrantless dragnet surveillance program violated the

---

[133] *Verizon Forces to Hand Over Telephone Data–Full Court Ruling*, The Guardian, June 5, 2013, http://www.guardian.co.uk/world/interactive/2013/jun/06/verizon-telephone-data-court-order.

[134] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN, June 6, 2013, http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order/ (originally published on June 5, 2013).

[135] Eagan Opinion, *supra* note 45, at 3.

[136] Ellen Nakashima & Scott Wilson, *ACLU Sues over NSA Surveillance Program*, WASH. POST, June 11, 2013, http://www.washingtonpost.com/politics/aclu-sues-over-nsa-surveillance-program/2013/06/11/fef71e2e-d2ab-11e2-a73e-826d299ff459_story.html.

[137] American Civil Liberties Union Complaint filed June 11, 2013, ACLU v. Clapper, No. 13-Civ-3994 (S.D.N.Y. 2013), *available at* https://www.aclu.org/files/assets/nsa_phone_spying_complaint.pdf.

[138] Nat'l Sec. Agency Telecommunications Records Litigation v. AT&T Corp., 671 F.3d 881, 890-91 (9th Cir. 2011).

[139] *Id.* at 891-92.

[140] Jewel v. NSA, 2013 U.S. Dist. LEXIS 103009 (N.D. Cal. July 23, 2013).

plaintiffs' Constitutional rights.[141] Although this case was based on leaked documentation of the alleged practices, unlike *Clapper*, the case was also originally dismissed on standing grounds.[142] However, the Ninth Circuit later reversed and allowed the plaintiffs standing to continue their suit.[143] Most recently, in July 2013, the U.S. District Court for the Northern District of California rejected the government's state secrets defense, allowing the plaintiff's First and Fourth Amendment claims to move forward.[144] The District Court did, however, conclude that the plaintiff's might have an uphill battle to overcome standing after *Clapper*:

> Although the Court finds, at this procedural posture, that Plaintiffs here do not allege the attenuated facts of future harm which barred standing in Clapper, the potential risk to national security may still be too great to pursue confirmation of the existence or facts relating to the scope of the alleged governmental Program.145

Similarly, in *CCR v. Obama*, the Ninth Circuit affirmed dismissal of a case challenging the Terrorist Surveillance Program, which ended in 2007.[146] The Court found that the plaintiffs lacked standing, much like the plaintiffs in *Clapper*,

> Although CCR might have a slightly stronger basis for fearing interception because of the lack of FISC involvement, CCR's asserted injury relies on a different uncertainty not present in [Clapper], namely, that the government retained 'records' from any past surveillance it conducted under the now-defunct TSP. In sum, CCR's claim of injury is largely factually

---

[141] *Id.* at *9-*11.

[142] Jewel v. NSA, 2010 U.S. Dist. LEXIS 5110 (N.D. Cal. Jan. 21, 2010).

[143] Jewel v. NSA, 673 F.3d 902 (9th Cir. 2011).

[144] Jewel v. NSA, 2012 U.S. Dist. LEXIS 176263 (N.D. Cal., Dec. 12, 2012), *as amended by Jewel, supra* note 140.

[145] Jewel, *supra* note 140, at *21.

[146] *In re* NSA Telecommunications Records Litigation, 522 F.App'x 383 (9th Cir. 2013). It is worth noting that the Terrorist Surveillance Program (TSP) only "ended" in the sense that the programs of interception constituting the warrantless TSP evolved into programs approved by the FISA Court, which largely kept their scope intact.

> indistinguishable from, and at least as speculative as, the claim rejected in [Clapper].147

In two recent district court decisions at the end of 2013, the District Court for D.C. and the District Court for the Southern District of New York came to opposite conclusions about the legality of the NSA's bulk telephone metadata surveillance activities.[148] These differing decisions may help bring the issue before the Supreme Court, which has recently declined to hear a case filed directly with the high court by the Electronic Privacy Information Center.[149] In the *ACLU v. Clapper* case, the plaintiffs overcame the standing issue that plagued Amnesty International USA in *Clapper v. Amnesty International USA*[150] because they could show, thanks to the Snowden disclosures, they were in fact the subjects of the government's phone call metadata surveillance. However, in reliance on the third party doctrine, the court concluded that telephone service subscribers maintained no legitimate expectation of privacy in their call metadata.[151] Conversely, in *Klayman v. Obama*, the court found that:

> [P]laintiffs have a very significant expectation of privacy in an aggregated collection of their telephony metadata covering the last five years, and the NSA's Bulk Telephony Metadata Program significantly intrudes on that expectation. Whether the program violates the Fourth Amendment will therefore turn on "the nature and immediacy of the government's concerns and the efficacy of the [search] in meeting them."[152]

---

147 *Id.* at 385.

148 *See* ACLU v. Clapper, 2013 WL 6819708 (S.D.N.Y. Dec. 27, 2013) (rejecting Fourth Amendment claims based on government telephone and metadata surveillance, but granting standing on metadata issue); Klayman v. Obama, 2013 WL 6571596 (D.D.C. Dec. 16, 2013) (finding NSA surveillance probably violates the Fourth Amendment, in suit alleging the government's PRISM program violated privacy and First Amendment rights).

149 *In re* Elec. Privacy Info. Ctr., 134 S.Ct. 638 (2013).

150 Clapper v. Amnesty Int'l USA, 133 S.Ct. 1138 (2013).

151 ACLU v. Clapper, 2013 WL 6819708, at *21-22.

152 Klayman v. Obama, 2013 WL 6571596, at *23 (citing Bd. of Educ. v. Earls, 536 U.S. 822, 834 (2002)).

In regards to the immediacy of the government's need for the surveillance, the court also found that:

> [T]he Government does *not* cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature. In fact, none of the three "recent episodes" cited by the Government that supposedly "illustrate the role that telephony metadata analysis can play in preventing and protecting against terrorist attack" involved any apparent urgency.[153]

However, despite this positive finding in favor of individual Fourth Amendment privacy, the court stayed its holding pending an appeal.[154]

These cases are far from the only challenges mounted by civil liberties organizations against government programs that mandated high levels of information secrecy. In just one additional example, although not a secret surveillance case *per se*, a Federal District Court judge held, in January 2013, that the United States government could keep information about its "targeted killing program" a secret.[155] In that case, the ACLU and New York Times had filed Freedom of Information Act lawsuits against the Department of Justice seeking information about the contested killing program. In her decision, Judge MacMahon stated that:

> The FOIA requests here in issue implicate serious issues about the limits on the power of the Executive Branch under the Constitution and laws of the United States, and about whether we are indeed a nation of laws, not of men. However….I can find no way around the thicket of laws and precedents that effectively allow the Executive Branch of our Government to proclaim as perfectly lawful certain actions that seem on their face

---

[153] *Id.* at *24.

[154] *Id.* at *26.

[155] N.Y. Times Co., v. U.S. Dept. of Justice, 2013 WL 50209 (S.D.N.Y. 2013).

> incompatible with our Constitution and laws, while keeping the reasons for its conclusion a secret.[156]

These cases demonstrate that U.S. courts are often exercising restraint when confronting challenges to the federal government's claims of secrecy in the name of national security. This restraint is in fairly sharp contrast to the willingness of the ECtHR to allow challenges and hold governments accountable for secret surveillance. (To be sure, the ECtHR has a different relationship to its relevant state governments than the Supreme Court has to the executive branch of the United States' government, but the difference in approaches and outcomes is still striking).

These situations clearly represent the nature and existence of potentially dominating activity by the state. As elaborated in the overall argument advanced in this paper, because the holdings effectively immunize the federal government from citizen review of the procedures and substance of government action they are highly suspect and problematic. In the very moments when these courts have been perfectly positioned to reduce government domination and protect the peoples' liberty, they have chosen to turn a blind eye or have a least been unwilling to robustly defend the Constitutional rights of American citizens.

V. LIBERTY: INTERFERENCE OR DOMINATION?

A. *Liberal Liberty: Berlin's Negative Conception of Freedom*

One of the most seminal essays in modern political philosophy on the topic of political liberty is Isaiah Berlin's *Two Concepts of Liberty*.[157] In that essay, Berlin outlines the trajectory of two different conceptions of liberty, what he calls "negative" and "positive" liberties. On one hand, negative liberty "is simply the area within which a [person] can act unobstructed by others."[158] A person's *degree* of freedom rests on whether, or how thoroughly, that person is prevented from doing something by another person.[159] A certain level

---

[156] *Id.* at *1.

[157] Isaiah Berlin, *Two Concepts of Liberty*, *in* LIBERTY: FOUR ESSAYS ON LIBERTY (Henry Hardy ed., 2d ed., 2002). For support of this claim, *see* ADAM SWIFT, POLITICAL PHILOSOPHY: A BEGINNER'S GUIDE FOR STUDENTS AND POLITICIANS 51 (2nd ed., 2006).

[158] Berlin, *supra* note 157, at 169.

[159] *Id.*

of interference by another with one person's freedom to do something, in Berlin's view, can equate to coercion or slavery, and thus ought to be avoided.[160] On the other hand, Berlin defines positive liberty as a form of self-mastery; to have one's decisions depend on no other person or any other force.[161] Despite some claims that this distinction (sometimes referred to as "freedom from" and freedom to") doesn't hold up,[162] Berlin provides an insightful tracing of the use of positive ideas about liberty that informed the development of totalitarian regimes like the Nazis and former USSR.[163]

Berlin's conception of negative liberty, however, has provided the basis for much contemporary work on philosophical liberty in the liberal tradition. Berlin himself noted that his version of negative liberty was not "logically…connected with democracy or self-government," although democratic self-government may admittedly guarantee liberty better than other forms of rule.[164] Berlin states "[t]he answer to the question 'Who governs me?' is logically distinct from the question 'How far does the government interfere with me?'"[165] Other writers have distinguished between "effective freedom" and "formal freedom," as a way to clarify Berlin's distinctions between positive and negative and to make the point that the absence of restraint (defined in terms of *legal* restraints) does not always guarantee the actual ability of and individual to do something he or she is legally entitled to do (for example, a person may not be able to take an expensive international vacation because of economic hardship).[166] On one hand, negative freedom is concerned with the absence of state restraint (or interference), while positive freedom is concerned about equalizing the effective freedoms of everyone is a society (e.g. international vacations might be assured by a state mandating a certain level of basic income). Some forms of positive freedom might also privilege the value of political engagement and

---

[160] *Id.*

[161] *Id.* at 178.

[162] SWIFT, *supra* note 157, at 52-54.

[163] *See generally* Berlin, *supra* note 157; SWIFT, *supra* note 157, at 51.

[164] Berlin, *supra* note 157, at 177.

[165] *Id.*

[166] *See, e.g.*, SWIFT, *supra* note 157, at 55.

self-government, as opposed to viewing laws as an interference (whether justified or not) on personal liberty.[167]

B. *Neorepublican Liberty: Pettit's Theory of Non-Domination*

In recent decades, republicanism, as an alternative to liberalism, has received renewed attention. Philip Pettit, a champion of one form of republicanism, often termed neorepublicanism or civic-republicanism, proposes a conceptualization of freedom as the opposite of "defenseless susceptibility to interference by another"–or put more simply, non-domination or "antipower."[168] This proposition is part of a larger neorepublican research agenda based on three primary tenets: individual freedom (conceptualized as freedom as nondomination), limited government power over its citizens based on a mixture of constitutionalism and the rule of law (with an emphasis on the importance of the free state promoting the freedom of its citizens without dominating them), and a vigilant commitment by citizens to preserve the freedom preserving structure and substance of their government through active democratic participation.[169]

Contrary to Berlin's account of negative liberty–that a person is free to the extent that no other entity actually interferes with that person's activity–Pettit's neorepublican position does away with the requirement of actual interference, focusing on eliminating the danger (or potential danger) of arbitrary interference from others.[170] Rather than predicating freedom on ideas of self-mastery, autonomy, or a person's ability to act in accordance with their higher-order desires,

---

[167] *Id.* at 64.

[168] Philip Pettit, *Freedom as Antipower*, 106 ETHICS 576, 576-77 (1996); Philip Pettit, *Republican Freedom and Contestatory Democratization*, *in* DEMOCRACY'S VALUE, 165 (I. Shapiro & C. Hacker-Cordon eds., 1999). *Cf.* PHILIP PETTIT, *REPUBLICANISM: A THEORY OF FREEDOM AND GOVERNMENT* (1997); PHILIP PETTIT, A THEORY OF FREEDOM: FROM THE PSYCHOLOGY TO THE POLITICS OF AGENCY (2001); Philip Pettit, *Keeping Republican Freedom Simple: On a Difference with Quentin Skinner*, 30 POL. THEORY 339 (2002); Philip Pettit, *Agency-Freedom and Option-Freedom*, 15 J. OF THEORETICAL POL. 387 (2003); Philip Pettit, *Freedom and Probability: A Comment on Goodin and Jackson*, 36 PHIL. AND PUBL. AFF. 206 (2008); Philip Pettit, *The Instability of Freedom as Noninterference: The Case of Isaiah Berlin*, 121 ETHICS 693 (2011); PHILIP PETTIT, ON THE PEOPLE'S TERMS: A REPUBLICAN THEORY AND MODEL OF DEMOCRACY (2012).

[169] Frank Lovett and Philip Pettit, *Neorepublicanism: A Normative and Institutional Research Program*, 12 ANN. REV. OF POL. SCI. 11 (2009).

[170] Frank Lovett, *Republicanism*, THE STANFORD ENCYCLOPEDIA OF PHILOSOPHY § 3.2, (Edward N. Zalta ed. Spring 2013), *available at* http://plato.stanford.edu/archives/spr2013/entries/republicanism/.

an account of Berlin's positive liberty, neorepublican theory is more concerned with ensuring the ability of the people to self-govern, by reducing domination and arbitrary interference.[171]

Pettit bases his account on the idea that the opposite of freedom is slavery (or the subjugation to arbitrary exercise of power).[172] Pettit is concerned that a conception of liberty limited to noninterference restricts our potential for appropriate emancipation from domination. Additionally, the noninterference view problematizes the application of law, as even general freedom preserving restrictions built into the rule of law constitute interference with absolute liberty (for example, the penalization of premeditated murder).

According to its proponents, this neorepublican political theory owes its origins to the experiences of the early Roman republic, and has been influenced and adopted by early figures such as Machiavelli, Jefferson, and Madison, and, more recently, by writers like Quentin Skinner and Philip Pettit,[173] although the precise historiography is still somewhat controversial.[174] Frank Lovett and Philip Pettit argue that their version of neorepublicanism has been adapted from what has been called "classical" republicanism to distinguish it from other, more communitarian, approaches.[175] Lovett also states that since political liberty ought to be "understood as a sort of structural relationship that exists between persons or groups, rather than as a contingent outcome of that structure," freedom is properly seen "as a sort of structural independence—as the condition of not being subject to the arbitrary power of a master."[176]

On another account, critical of Pettit's emphasis on nondomination as the core ethical-political commitment of

---

[171] *Id.*

[172] *See* Pettit, *Freedom as Antipower*, *supra* note 168, at 576; Lovett, *supra* note 170, at § 1.2.

[173] Lovett, *supra* note 170, at § 3.1; Quentin Skinner, LIBERTY BEFORE LIBERALISM (1998); Quentin Skinner, *The Republican Ideal of Political Liberty*, *in* MACHIAVELLI AND REPUBLICANISM (G. Bock, Q. Skinner, & M. Viroli eds. 1998), 239-309; *see also* Z.S. FINK, THE CLASSICAL REPUBLICANS: AN ESSAY IN THE RECOVERY OF A PATTERN OF THOUGHT IN SEVENTEENTH CENTURY ENGLAND (1945); C. ROBBINS, THE EIGHTEENTH-CENTURY COMMONWEALTHMAN (1959); J.G.A. POCOCK, THE MACHIAVELLIAN MOMENT: FLORENTINE POLITICAL THOUGHT AND THE ATLANTIC REPUBLICAN TRADITION (1979); M.N.S. SELLERS, AMERICAN REPUBLICANISM: ROMAN IDEOLOGY IN THE UNITED STATES CONSTITUTION (1994).

[174] Lovett, *supra* note 170, at § 1.

[175] *See* Lovett and Pettit, *supra* note 169.

[176] Lovett, *supra* note 170, at § 1.2.

republicanism itself, "domination should be seen as the expression of oligarchic (and even tyrannical) concentrations of power within society as a whole, as pathological results of a badly arranged society."[177] On this account, we should be concerned not only with limiting the arbitrary domination of some, and:

> [T]he emphasis should be placed on the ways in which the freedom of individual agents is rooted in the structure of social power as a whole: in ensuring that society is arranged in such a way as to orient social power not only negatively, but positively as well.[178]

Thus, power and domination are built into the structure of social institutions, and this structure, if constructed improperly, potentially allows institutions to dominate and subjugate the people systemically. This, in turn, makes it difficult for "individuals and groups to possess political control over the institutions which govern their lives," a serious problem for republican politics.[179] Domination, then, can become institutionalized and integrated into our social and political institutions in a way that creates systemic domination,[180] as well as evidenced in the relationships between agents of government and individuals or groups of citizens.

But what exactly is domination, from the neorepublican position? Domination requires the capacity to interfere, with impunity and in an arbitrary fashion, with certain choices that the dominated agent otherwise has the capacity to make. I say "certain choices" because the scope of the interference need not impinge on all of the dominated agent's choices, but may be limited to just a subset of choices of varying centrality or importance. Interference requires "an intentional attempt to worsen an agent's situation of choice.[181] Unintentional or accidental interference is not freely exercised subjugation. However, interference does encompass a wide amount of possible actions, including restraint, obstruction, coercion, punishment (or threat of

---

[177] Michael J. Thompson, Reconstructing Republican Freedom: A Critique of the Neo-Republican Concept of Freedom as Non-Domination, 39 PHILOSOPHY SOCIAL CRITICISM 277, 278 (2013).

[178] *Id.*

[179] *Id.* at 279.

[180] *Id.* at 290.

[181] Philip Pettit, *Freedom as Antipower, supra* note 168, at 578.

punishment), and manipulation (which includes, in Pettit's view, "agenda fixing, the deceptive . . . shaping of people's beliefs or desires, [and] rigging . . . the consequences of people's actions").[182]

Thus, this sort of interference worsens the dominated agent's position–and causes damage–because it changes the options available to the person or alters the payoffs of the person's choices by allowing the subjugator to manipulate the options and payoffs in play. In this sense, the power-wielding agent has the necessary capacity to interfere. The agent must also be capable of interfering with impunity and at will (or arbitrarily) in order to fully dominate the other. This condition requires that the agent act without risk of penalty for interfering–whether from the victim themselves (directly or indirectly) or society at large. If these criteria are satisfied, then the agent has "absolutely arbitrary power."[183] The only check on the exercise of such power is in the agent itself–in that agent's free and capricious will. Thus, it follows that a person (X) is dominated by another (Y) when X has no legal recourse to contest actions by Y that interfere with X's situation of choice. Thus, because widespread state surveillance of the communications of its citizens has the potential to interfere with individual citizens' situations of choice (for example, by chilling free expression), this relationship exhibits domination.

In response to this conception of domination as the antithesis of liberty, the neorepublican project places a great premium on emancipation–through balancing power and limiting arbitrary discretion–and active political participation. Importantly, reversing roles would not solve the problem of domination, but would merely relocate it.[184] Fairly allocating power to both sides, on the other hand, does not just merely equalize the subjugation; if both sides–say the people and their government–may interfere with the other's affairs, then neither may act with impunity since the other may exact something in return.[185] Thus, "neither dominates the other."[186] This is an exemplification of what Pettit terms "antipower."[187] According to Pettit, "Antipower is what comes into being as the power of some over others–the power of some over others in the sense associated with

---

[182] *Id.* at 579.

[183] *Id.* at 580.

[184] *Id.* at 588.

[185] *Id.*

[186] *Id.*

[187] See Pettit, Freedom as Antipower, supra note 168.

domination–is actively reduced and eliminated."[188] Antipower, then, subjugates power and, as a form of power itself, allows persons to control the nature of their own destiny.[189] In this sense, the "person enjoys the noninterference resiliently" because they are not dependent on the arbitrary use of power, precisely because they have the power to "command noninterference."[190]

One way to provide a citizenry with the power to command noninterference is to regulate the resources of the powerful, which might include checks on and separations of power, regular representative elections, democratic participation, limited tenure of government officials, access to independent courts or other bodies with powers to review government action, and open access to information.[191] Because access to information is a prerequisite to seeking legal recourse for potentially dominating activities of another, this aspect of power regulation should take an important place in our domestic and international information policies.

Of course, as Pettit's neorepublican project concedes, fully eliminating domination may not be always be easy, or even completely possible, and antipower may exist to varying degrees. Commanding noninterference may require collective action, and this theory admittedly relies on the presence of institutions as means to administer government and facilitate the peoples' claims. This does not mean, however, that we ought to be complacent, or even limit our concern to reducing actual interference. On the contrary, if an act or policy of an institution or agent of government arbitrarily dominates the will and autonomy of citizens, thus violating their ability to self-govern, then these acts or policies and are unjustified and ought to be corrected.

Thus, under this neorepublican conception of liberty, the proposition that governments must allow their citizens enough access to information necessary for individual self-government is entirely appropriate. To be fully non-arbitrary and non-dominating, government must also respect and provide effective institutional and legal mechanisms for their citizenry to effectuate self-government and command noninterference. Establishing liberal access rights to information about government conduct and mechanisms that ensure that citizens can effectively command noninterference are justified on

---

[188] *Id.* at 588.

[189] *Id.* at 589.

[190] *Id.*

[191] *Id.* at 591.

the grounds that they reduce the possibility of arbitrary, and actual, interference with the right of the people govern themselves. Such measures would also limit the institutionalization of systemic domination within political and social institutions, as Thompson fears.[192]

VI. CONCLUSION

Government surveillance can be detrimental to individual liberty.[193] It may chill the exercise of civil liberties, such as free speech,[194] or may violate subjective and/or objective expectations of privacy that ought to be protected under the Fourth Amendment. Secret surveillance laws pose a danger of "undermining or even destroying democracy on the ground of defending it" in their "struggle against espionage and terrorism."[195] In the aggregate, databases of personal information provide the government with the opportunity to conduct longitudinal analysis of individual citizens' behavior and communication practices, and may result in sophisticated statistical analysis, including the forecasting of future action based on past events.

On Berlin's negative account of liberty, a person is free if she does not actually suffer interference: if she is not subjected to manipulation, coercion, threat, or compulsion. This view is indeed attractive. Can we really say that a person is less free to express themselves when no one ever actually interferes with their speech (despite the possibility, however vague and unlikely) than when no one *can* interfere at all? The noninterference view of freedom has been embraced by some, like Hobbes, Paley, and Bentham, to argue that that all law and every form of government restricts liberty.[196]

On the other hand, viewing freedom as antipower–as the absence of domination by another–allows us to respect the importance of noninterference in many cases, but also recognizes that the non-voluntary nature of the rule of law (with opportunities for effective

---

[192] *See* Thompson, *supra* note 177.

[193] *See* FORCESE & FREEMAN, *supra* note 1; Neil Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1934-35 (2013).

[194] Richards, *supra* note 193, at 1935.

[195] FORCESE & FREEMAN, *supra* note 1, at 49.

[196] Pettit, *Freedom as Antipower*, *supra* note 168, at 598-600; Lovett & Pettit, *supra* note 166, at 13-15.

appeal and democratic participation) actually protects and preserves our freedoms, rather than restricting them as a means to some other end. A person living under a friendly despot is not in the same position–in terms of freedom–as the person living in a properly constituted constitutional democracy with limits on domination. Fully realizing a situation of more equalized reciprocal surveillance and rights to access and document information about government activities (with temporary exceptions as may be needed to protect national security) would give citizens greater ability to ensure their government was not overreaching and abusing its authority, to hold the state and state actors accountable for rights violations, and to maintain government as an entity that protects it citizens' freedoms without coming to subjugate them to arbitrary exercises of power.

Strict limitations on standing in cases challenging secret government surveillance activities constitute an interference with individual freedom, as the ECtHR has held.[197] The stark differences in the ability of plaintiffs to claim violations of their constitutional or basic human rights in the U.S. and at the ECtHR, provides a suggestive critique of the nature of the current judicial politics of surveillance and transparency in domestic U.S. courts. The unwillingness of U.S. courts to allow challenges to secret government surveillance programs on standing grounds is a failure of the judicial system to check the ability of the executive to usurp arbitrary domination over the people. It is a failure of antipower in America.

The primary point of this argument, then, is not that we eliminate or unduly restrict to ability of government and law enforcement to conduct surveillance (or to restrict access to certain information in some cases), but rather that we recognize the bargain we have struck, in our representative democratic society, that the government assume some surveillance powers–and thus encroach on our individual negative freedoms to some degree–because they have the ability (and the responsibility) to use these powers for the public good. Our contract, and our consent, does not negate the possibility of domination or the relevance of freedom (including its attendant needs for personal privacy and free speech).[198] However, this power cannot be granted without strings attached.

Information can (and does) provide and facilitate power. Significantly, the collection and use of large amounts of information (including communications metadata) can significantly impact the

---

[197] *Id.*

[198] Pettit, *Freedom as Antipower*, *supra* note 168, at 585.

relationships between governments and their citizens.[199] Because access to information is often a prerequisite to exercising power or seeking redress for potential rights violations stemming from secret activities of others,[200] we must allow challenges to secrecy in government that tip the balance of information access to far too one side. An imbalance in information access between a people and their government will tip the scales of power and limit the ability of the people to exercise democratic oversight and control those they have put in power to represent them.[201] Freedom of information laws provide one way to access to government records and serve as a powerful and effective means for empowering oversight by journalists and ordinary citizens. These laws, which provide a legal mechanism for citizen-initiated reciprocal-surveillance must capture more information about the legal bases and secret surveillance programs to ensure that "adequate and effective guarantees against abuse"[202] exist. This form of reciprocal surveillance will grant citizens greater power to check government abuse and force even greater transparency.[203] Otherwise, our privacy and liberty risk becoming a "nullity."[204] The violation of our rights should not hinge on our *awareness* of government overreaching, but whether the government has in fact acted impermissibly, visibly or in secret. As such, our access to remedies (and information) should not similarly be limited solely to cases involving non-secret government action.

To preserve our freedom, we must also act to ensure our freedoms are protected; we must use the channels of democratic participation available to us to effectuate our own nondomination. These channels might include political participation, litigation, exercising our free speech rights, or documenting government conduct in various ways, such as through filming public officials exercising their public duties in public spaces or filing freedom of information requests to uncover suspected wrongdoing. We should not be forced to grant our government the ability to exercise its powers arbitrarily, without oversight, especially when those powers have the ability to limit our freedoms. Implementing and maintaining greater checks on the

---

[199] *See* FORCESE & FREEMAN, *supra* note 1, at 481-84.

[200] *Id.*

[201] *Id.*

[202] *Klass*, *supra* note 54, at para. 50.

[203] Brin, *supra* note 6; Haggarty and Ericson, *supra* note 6, at 10.

[204] *Klass*, *supra* note 54, at para. 36.

exercise of government surveillance powers would remove the opportunity for subjugation, enable an important emancipation from information secrecy, and promote individual liberty.