6-2018

Bulk Biometric Metadata Collection

Margaret Hu

BULK BIOMETRIC METADATA COLLECTION*

MARGARET HU**

Smart police body cameras and smart glasses worn by law enforcement increasingly reflect state-of-the-art surveillance technology, such as the integration of live-streaming video with facial recognition and artificial intelligence tools, including automated analytics. This Article explores how these emerging cybersurveillance technologies risk the potential for bulk biometric metadata collection. Such collection is likely to fall outside the scope of the types of bulk metadata collection protections regulated by the USA FREEDOM Act of 2015. The USA FREEDOM Act was intended to bring the practice of bulk telephony metadata collection conducted by the National Security Agency ("NSA") under tighter regulation. In the wake of the disclosures by Edward Snowden in June 2013, members of Congress called for statutory reform to eliminate or significantly curtail indiscriminate metadata surveillance of United States citizens. The Snowden revelations illuminated that the bulk telephony metadata collection program had been legally justified under Section 215 of the USA PATRIOT Act. This Article contends that the USA FREEDOM Act, which amended Section 215 of the USA PATRIOT Act, does not restrict other types of non-telephony bulk metadata collection. This Article concludes that, rather than more tightly regulating metadata surveillance, the Act allows for metadata surveillance to proceed under differing justifications and in more delegated contexts. The potential of ubiquitous and continuous data collection and analysis that may stem from smart body cameras or smart glasses worn by law enforcement offers an important case study on why

** Margaret Hu, Associate Professor of Law, Washington and Lee University School of Law. This Article greatly benefitted from helpful discussions with David Ardia, Andrew Christensen, Bart Forsyth, Jennifer Granick, Tim Keefer, Rachel Levinson-Waldman, Peter Margulies, Richard Myers, Faiza Patel, and Peter Swire, who all generously shared their expertise. My deepest gratitude to the *North Carolina Law Review* for hosting the 2017 Symposium, "Badge Cams as Data and Deterrent: Law Enforcement, the Public and the Press in the Age of Digital Video," and to Rebecca Neubauer for her editorial care. Many thanks to Rossana Baeza, Emily Bao, Mark Dewyea, Kirby Kreider, and Carroll Neale for their excellent research assistance.

the USA FREEDOM Act is unable to regulate bulk biometric metadata collection.

INTRODUCTION

In the contemporary market, police body cameras are generally understood to be first-generation technologies that execute one-dimensional surveillance capacities.[1] For example, most police body cameras available on the market are currently designed to store the audio-video recording of images captured in average definition through manual operation, subject to data storage limitations.[2] Yet, a

1. A great deal of important scholarship has been produced on the legal and policy consequences of police body cameras in recent years. *See, e.g.*, Kami N. Chavis, *Body-Worn Cameras: Exploring the Unintentional Consequences of Technological Advances and Ensuring a Role for Community Consultation*, 51 WAKE FOREST L. REV. 985, 987–89 (2016); Mary D. Fan, *Privacy, Public Disclosure, Police Body Cameras: Policy Splits*, 68 ALA. L. REV. 395, 397–401 (2016).

2. Mary D. Fan, *Justice Visualized: Courts and the Body Camera Revolution*, 50 U.C. DAVIS L. REV. 897, 901 (2017) ("Small enough to be worn on the head, ear, or chest, a body camera can go everywhere officers go, providing audiovisual recording of what officers see, hear and do.") (citing NAT'L INST. OF JUSTICE, A PRIMER ON BODY-WORN CAMERAS FOR LAW ENFORCEMENT 5-6 (2012), https://www.justnet.org/pdf/00-Body-Worn-Cameras-508.pdf [http://perma.cc/3PYS-EL9M]). Body-worn cameras have been defined as "a small audio-video recorder with the singular purpose of recording audio/visual files, specifically designed to be mounted on a person." *Id.* at 901 n.15 (citing S.F. POLICE DEP'T, BODY WORN CAMERAS POLICY, RECOMMENDED DRAFT 1 (2015), http://sanfranciscopolice.org/sites/default/files/FileCenter/Documents/27674-BWC%20VERSION%201.pdf [http://perma.cc/4VM3-U6RW]).

next generation of smart police body cameras increasingly attempt to integrate live-streaming video with facial recognition and other artificial intelligence tools, such as automated analytics and database screening capacities.[3] Similarly, smart glasses, if and when they are worn by law enforcement on a broad scale, will have the potential to facilitate a wide range of data sensor and analytic capacities.[4]

Consequently, the emerging cybersurveillance capacities of smart police body cameras and smart glasses are not fully appreciated.[5] This Article explores how these technologies facilitate biometric cybersurveillance[6] through the capture and storage of biometric data such as facial images.[7] According to one study, digital images of 117

3. *See, e.g.*, Alex Pasternack, *Police Body Cameras Will Do More Than Just Record You*, FAST COMPANY (Mar. 3, 2017), https://www.fastcompany.com/3061935/police-body-cameras-livestreaming-face-recognition-and-ai [http://perma.cc/8NLQ-L3M].

4. *See, e.g.*, Jeremy Hsu, *Face of the Future: How Facial-Recognition Tech Will Change Everything*, NBC NEWS (June 11, 2013, 4:49 PM), http://www.nbcnews.com/id/52172415/ns/technology_and_science-tech_and_gadgets/t/face-future-how-facial-recognition-tech-will-change-everything/#.WpGZ0e7wZjQ [http://perma.cc/CY8L-NBJK]; Jon Russell, *Chinese Police are Using Smart Glasses to Identify Potential Suspects*, TECHCRUNCH (Feb. 8, 2018), https://techcrunch.com/2018/02/08/chinese-police-are-getting-smart-glasses/ [http://perma.cc/2RLZ-6X4A].

5. For other important scholarship on surveillance, see, for example, Julie Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1931 (2013) (asserting that "[p]rotection against government surveillance is necessary if we are to avoid an Orwellian surveillance society"); Ashley S. Deeks, *Intelligence Agencies and International Law*, 102 VA. L. REV. 599, 617 (2016) ("Other [governmental] activities stimulate far more concern, however, particularly when those activities directly implicate the life, liberty, and privacy of individuals not associated with governments. The recent [Snowden] leaks have illustrated—in ways that startled the general public—the prevalence today of that latter type of activity."); Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 528 (2017) ("Where law enforcement is involved, these powerful new technologies also raise questions about how their use can be harmonized with the U.S. Constitution."); Neil Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1934 (2013) ("Although we have laws that protect us against government surveillance, secret government programs cannot be challenged until they are discovered. And even when they are, our law of surveillance provides only minimal protections.").

6. *See, e.g.*, Margaret Hu, *Biometric ID Cybersurveillance* 88 IND. L.J. 1475, 1477 n.3; *see also id.* at 1480 n.15 (defining cybersurveillance as "the process by which some form of human activity is analyzed by a computer according to some specified rule. . . . [T]he critical feature in each [case of surveillance] is that a computer is sorting data for some follow-up review by some human." (quoting LAWRENCE LESSIG, CODE VERSION 2.0, at 209 (2006)).

7. *The Current and Future Applications of Biometric Technologies: Joint Hearing Before the Subcomm. on Research & Subcomm. on Tech. Comm. On Sci., Space and Tech.*, 113th Cong. 16 (2013) [hereinafter Romine Testimony] (statement of Charles H. Romine, Director, Information Technology Laboratory, National Institute of Standards and Technology) ("Biometric technologies can provide a means for uniquely recognizing humans based upon one or more physical or behavioral characteristics and can be used to

million individuals, criminals and non-criminals, are already stored in a searchable federal, state, or local database.[8] What may be less understood, however, is how biometric data collection also includes "associated metadata [collection]—information about the biometric characteristics or how [the biometric data] was collected."[9] This Article, therefore, focuses on one risk associated with these emerging surveillance technologies: the potential for bulk biometric metadata collection, a practice which is likely to fall outside of the scope of the types of bulk metadata collection protections regulated by the USA FREEDOM Act.[10]

Metadata is data about data, which includes for example the time of a telephone call or the email addresses of a recipient and sender.[11] The USA FREEDOM Act of 2015 was intended to bring the practice of bulk telephony metadata collection conducted by the NSA under tighter regulation.[12] In the wake of the disclosures by Edward

establish or verify personal identity of individuals previously enrolled. Examples of physical characteristics include face photos, fingerprints, and iris images.").

8. Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America,* GEO. L. CTR. ON PRIVACY & TECH. (Oct. 18, 2016), https://www.law.georgetown.edu/news/press-releases/half-of-all-american-adults-are-in-a-police-face-recognition-database-new-report-finds.cfm [http://perma.cc/833X-ZWQY].

9. *New NIST Biometric Data Standard Adds DNA, Footmarks and Enhanced Fingerprint Descriptions,* NAT'L INST. SCI. & TECH. (Dec. 6, 2011), https://www.nist.gov/news-events/news/2011/12/new-nist-biometric-data-standard-adds-dna-footmarks-and-enhanced [https://perma.cc/BW77-8YSW].

10. USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (codified at 50 U.S.C. 1801 (2016)).

11. *See, e.g.*, OFFICE OF THE PRIVACY COMM'R OF CAN., METADATA AND PRIVACY: A TECHNICAL AND LEGAL OVERVIEW 1 (2014), https://www.priv.gc.ca/media/1786/md_201410_e.pdf [https://perma.cc/HXA7-ES6V] ("Simply put, metadata is data that provides information about other data. It is information that is generated as you use technology.").

12. In an early version of the USA FREEDOM Act, the language of the statute stated the following purpose: "To rein in the dragnet collection of data by the National Security Agency (NSA) and other government agencies, increase transparency of the Foreign Intelligence Surveillance Court (FISC), provide businesses the ability to release information regarding FISA requests, and create an independent constitutional advocate to argue cases before the FISC." *See* Alex Byers, *Surveillance Reform Bill Outlined*, POLITICO (Oct. 2, 2013), https://www.politico.com/blogs/under-the-radar/2013/10/surveillance-reform-bill-outlined-174157 [https://perma.cc/4YDR-VKXS] (quoting USA FREEDOM Act, H.R. 3361, 113th Cong. (2013); S. 1599, 113th Cong. (2013)). The original acronym for the USA FREEDOM Act was Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act. Dan Roberts, *The USA FREEDOM Act: A Look at the Key Points of the Draft Bill*, GUARDIAN (Oct. 10, 2013, 5:16 PM), http://www.theguardian.com/world/2013/oct/10/the-usa-freedom-act-a-look-at-the-key-points-of-the-draft-bill [https://perma.cc/8CN6-ZSSL] ("The bill has a somewhat cumbersome title: [T]he Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-

Snowden in June 2013,[13] members of Congress immediately called for statutory reform to eliminate or significantly curtail indiscriminate telephony metadata surveillance of U.S. citizens.[14] Congressman James Sensenbrenner (R-Wisc.), former Chair of the House Judiciary Committee and a sponsor of the Act, explained that the Snowden disclosures had revealed an intelligence community program that had, in his opinion, clearly exceeded the boundaries of the intent of the underlying law that had been used by the NSA to justify it: the USA PATRIOT Act of 2001.[15] According to Congressman Sensenbrenner—one of the original architects of the USA PATRIOT Act[16]—the practice of mass, suspicionless collection of the metadata of every phone call by millions of Verizon subscribers daily for a period of several years was not within the type of intelligence activity that had been authorized, or even anticipated, by the USA

Collection and Online Monitoring Act. But it's one of those pieces of legislation that has been named for its acronym: the USA FREEDOM Act."). The USA FREEDOM Act was modified in House Resolution 2048, sponsored by Congressman Sensenbrenner, to reflect the following title: "Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act." Pub. L. No. 114-23, § 1, 129 Stat. at 268.

13. *See, e.g.*, H.R. REP. NO. 114-891 (2016); Barton Gellman, Aaron Blake & Greg Miller, *Edward Snowden Comes Forward as Source of NSA Leaks*, WASH. POST (June 9, 2013), https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html?utm_term=.8e92cf79c0ed [https://perma.cc/3E2Z-5S5K].

14. *See, e.g.*, Press Release, Office of Sen. Ron Wyden, Wyden, Udall Statement on the Disclosure of Bulk Email Records Collection Program (July 2, 2013), https://www.wyden.senate.gov/news/press-releases/wyden-udall-statement-on-the-disclosure-of-bulk-email-records-collection-program [https://perma.cc/HJ35-KS84]; Press Release, Office of Sen. Ron Wyden, Wyden and Udall: Intelligence Community's Response Leaves Important Surveillance Questions Unanswered (July 26, 2013), https://www.wyden.senate.gov/news/press-releases/wyden-and-udall-important-surveillance-questions-unanswered [https://perma.cc/QJ6Q-9Y8E]; Ellen Nakashima, *Sen. Patrick Leahy Calls for End to NSA Bulk Phone Records Program*, WASH. POST (Sept. 24, 2013), https://www.washingtonpost.com/world/national-security/sen-patrick-leahy-calls-for-end-to-nsa-bulk-phone-records-program/2013/09/24/85a21f66-252a-11e3-b3e9-d97fb087acd6_story.html [https://perma.cc/L55Y-BTZE].

15. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, sec. 215, § 501, 115 Stat. 272, 287 (codified as amended at 50 U.S.C. § 1861 (2012)). *See* Matt Fuller, *Sensenbrenner Slams NSA to European Parliament*, ROLL CALL (Nov. 11, 2013, 11:55 AM), http://www.rollcall.com/218/sensenbrenner-slams-nsa-to-european-parliament [https://perma.cc/24AC-TUXU]; Jim Sensenbrenner, *NSA Abused Trust, Must Be Reined in*, MILWAUKEE J. SENTINEL (Nov. 2, 2013), http://www.jsonline.com/news/opinion/nsa-abused-trust-must-be-reined-in-b99131601z1-230292131.html [https://perma.cc/SPR8-W6LY] ("It ignored restrictions painstakingly crafted by lawmakers and assumed a plenary authority never imagined by Congress.").

16. *See, e.g.*, *Patriot Act Architect Criticizes NSA's Data Collection*, NAT'L PUB. RADIO (Aug. 20, 2013, 5:22 PM), http://www.npr.org/templates/story/story.php?storyId=213902177 [https://perma.cc/G8DV-P42B (dark archive)].

PATRIOT Act.[17] The USA FREEDOM Act was intended to address what Congress perceived as a significant loophole in the USA PATRIOT Act that had allowed for bulk metadata collection.[18]

With the election of President Donald J. Trump, commentators have placed greater attention on how the Trump administration will access and utilize tools of mass surveillance to achieve national security objectives.[19] Administration officials have called for the return of bulk metadata collection.[20] Understanding the limitations of the USA FREEDOM Act can illuminate why bulk metadata surveillance may likely be expanded.

17. *Id.* ("What Congress intended and what I intended is that the target had to be a foreign national and not a U.S. person. He would be targeted, and then they would find out who that person was calling, both in the United States and elsewhere, rather than grabbing all of the phone information and working backwards to the target." (quoting statement of Congressman Jim Sensenbrenner)); *see also* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013, 6:05 AM), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [https://perma.cc/F7S2-LMD5].

18. *See Patriot Act Architect Criticizes NSA's Data Collection, supra* note 16.

19. Spencer Ackerman & Sabrina Siddiqui, *Trump v US Intelligence: Growing Feud Puts NSA's Legislative Priority at Risk*, GUARDIAN (Mar. 7, 2017), https://www.theguardian.com/us-news/2017/mar/07/trump-nsa-us-intelligence-prism-reauthorization [https://perma.cc/37RR-TXYA]; Andy Greenberg, *Just in Time for Trump, the NSA Loosens its Privacy Rules*, WIRED (Jan. 12, 2017, 4:25 PM), https://www.wired.com/2017/01/just-time-trump-nsa-loosens-privacy-rules/ [https://perma.cc/2EHN-QB5J]; Andy Greenberg, *Imagine if Donald Trump Controlled the NSA*, WIRED (Oct. 19, 2016, 7:00 AM), https://www.wired.com/2016/10/imagine-donald-trump-controlled-nsa/ [https://perma.cc/L4D3-Z2MB]; Chris Strohm, *FBI and NSA Poised to Gain New Surveillance Powers Under Trump*, BLOOMBERG TECH. (Nov. 29, 2016, 5:00 AM), https://www.bloomberg.com/news/articles/2016-11-29/fbi-and-nsa-poised-to-gain-new-surveillance-powers-under-trump [https://perma.cc/N6M4-MNGA (dark archive)].

20. Mike Pompeo & David B. Rivkin, Jr., *Time for a Rigorous National Debate About Surveillance*, WALL ST. J. (Jan. 3, 2016, 4:21 PM), https://www.wsj.com/articles/time-for-a-rigorous-national-debate-about-surveillance-1451856106 [https://perma.cc/M76W-HECP (dark archive)].

> Congress should pass a law re-establishing collection of all metadata, and combining it with publicly available financial and lifestyle information into a comprehensive, searchable database. Legal and bureaucratic impediments to surveillance should be removed. That includes Presidential Policy Directive-28, which bestows privacy rights on foreigners and imposes burdensome requirements to justify data collection.

Id.; *see also* Jonathan Landay, *Trump's CIA Pick Supports Domestic Surveillance, Opposes Iran Deal*, REUTERS (Nov. 18, 2016, 7:18 PM), http://www.reuters.com/article/us-usa-trump-pompeo-newsmaker-idUSKBN13D2HM [https://perma.cc/2B25-BBCG]; Kaveh Waddell, *Trump's CIA Director Wants to Return to a Pre-Snowden World*, ATLANTIC (Nov. 18, 2016), https://www.theatlantic.com/technology/archive/2016/11/trumps-cia-director-wants-to-return-to-a-pre-snowden-world/508136/ [https://perma.cc/ZS7F-U4WG].

The USA FREEDOM Act, although a legislative achievement[21] that embodies a tremendous cooperative bipartisan political effort,[22] cannot be understood as a statute that regulates bulk metadata collection generally. Specifically, the USA FREEDOM Act is an achievement in that it forced Congress to meaningfully confront the role of proper legislative oversight in regulating the metadata surveillance activities of the NSA[23] at the dawn of the big data revolution.[24] Yet, this Article argues, rather than more tightly

21. Jennifer Steinhauer & Jonathan Weisman, *U.S. Surveillance in Place Since 9/11 is Sharply Limited*, N.Y. TIMES (June 2, 2015), http://www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-but-showdown-looms.html [https://perma.cc/ZS7F-U4WG (dark archive)] ("The legislation signaled a cultural turning point for the nation, almost 14 years after the Sept. 11 attacks heralded the construction of a powerful national security apparatus. The shift against the security state began with the revelation by Edward J. Snowden, a former [NSA] contractor, about the bulk collection of phone records.").

22. *See, e.g.*, Presidential Statement on Congressional Passage of the USA FREEDOM Act, 2015 DAILY COMP. PRES. DOC. 412 (June 2, 2015) ("I particularly applaud Senators Leahy and Lee as well as Representatives Goodlatte, Sensenbrenner, Conyers, and Nadler for their leadership and tireless efforts to pass this important bipartisan legislative achievement."); Steinhauer & Weisman, *supra* note 21 ("The battle over the legislation, the USA [FREEDOM] Act, made for unusual alliances. Mr. Boehner joined forces with Mr. Obama, the bipartisan leadership of the House Judiciary Committee, and a bipartisan coalition of senators against Mr. McConnell and his Intelligence Committee chairman, Senator Richard Burr, Republican of North Carolina.").

23. *See, e.g.*, William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEX. L. REV. 1633, 1634–36 (2010); Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721, 1755–58 (2014). *See generally* LAURA K. DONOHUE, THE FUTURE OF INTELLIGENCE: PRIVACY AND SURVEILLANCE IN A DIGITAL AGE (2016) (tracing the evolution of U.S. foreign intelligence law and pairing it with the progress of Fourth Amendment jurisprudence); Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J. L. & PUB. POL'Y 117 (2015) [hereinafter Donohue, *Section 702*] (analyzing the evolution of section 702 of the Foreign Intelligence Surveillance Act Amendments Act, statutory issues related to upstream collection, and constitutional concerns accompanying these issues); Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J. L. & PUB. POL'Y 757 (2014) [hereinafter Donohue, *Bulk Metadata Collection*] (examining the bulk collection of metadata under the authority of the Foreign Intelligence Surveillance Act and related constitutional concerns); Peter Margulies, *Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection After Snowden*, 66 HASTINGS L.J. 1 (2014) (arguing for a more public advocate to hold FISC accountable in its decision making); Nathan Alexander Sales, *Domesticating Programmatic Surveillance: Some Thoughts on the NSA Controversy*, 10 I/S: J.L. & POL'Y FOR INFO. SOC'Y 523 (2014) (examining NSA programs and their benefits and drawbacks); Patrick Toomey & Brett Max Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants, & the Right to Notice*, 54 SANTA CLARA L. REV. 843 (2014) (discussing the requirement of notice as it applies to NSA's secret use of electronic surveillance);

24. VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 157 (2013)

regulating metadata surveillance, the USA FREEDOM Act allows for metadata surveillance to proceed under differing justifications and through more delegated contexts.[25] As will be discussed below, bulk biometric metadata collection, for instance, can occur through corporate surveillance products contracted or acquired by homeland security and law enforcement organizations. The federal government could delegate collection to state and local law enforcement through cooperative data sharing, for example, of live-streaming video and other data collected by smart police body cameras or smart glasses.

This Article proceeds in three parts. Part I sets forth how police body cameras will likely create a vehicle for mass biometric collection generally and bulk biometric metadata collection specifically. This Part, by way of comparison, describes data garnered from the bulk telephony surveillance of telecommunications and the bulk biometric data facial imagery recognition. Part I then argues that the mass amount of data derived from body-camera surveillance initiatives has the potential to facilitate database compilation and interagency sharing at the federal level. It explains how this data collection and sharing will not be subject to effective oversight due to a lack of meaningful legal restrictions or administrative walls barring data sharing within the intelligence community or between federal and state or local law enforcement entities. Part I discusses the nature of cooperative data sharing between and among the U.S. Department of

("When the collection expands to information like financial transactions, health records, and Facebook status updates, the quantity being gleaned is unthinkably large."); *see also* Mark Andrejevic, *Surveillance in the Big Data Era*, *in* EMERGING PERVASIVE INFORMATION AND COMMUNICATION TECHNOLOGIES (PICT): ETHICAL CHALLENGES, OPPORTUNITIES AND SAFEGUARDS 55, 56 (Kenneth D. Pimple ed., 2014) ("[I]n the era of 'big data' surveillance, the imperative is to monitor the population as a whole: otherwise it is harder to consistently and reliably discern useful patterns."); David Lyon, *Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique*, BIG DATA & SOC'Y, July 2014, at 1, 2 ("[A]s political-economic and socio-technological circumstances change, so surveillance also undergoes alteration, sometimes transformation."); Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 241 (2013) ("The Obama Administration has recently announced a new, multi-agency big data research and development initiative aimed at advancing the core scientific and technological means of managing, analyzing, visualizing, and extracting information from large, diverse, distributed, and heterogeneous data sets."). *See generally* JULES J. BERMAN, PRINCIPLES OF BIG DATA: PREPARING, SHARING, AND ANALYZING COMPLEX INFORMATION (2013) (explaining Big Data design and analysis); ROB KITCHIN, THE DATA REVOLUTION: BIG DATA, OPEN DATA, DATA INFRASTRUCTURES & THEIR CONSEQUENCES (2014) (discussing the various principles of Big Data); PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT (Julia Lane et al. eds., 2014) (providing conceptual, practical, and statistical frameworks for analyzing emergent issues related to the data revolution).

25. *See infra* Parts I.C, II.B.

Homeland Security ("DHS") and between state, local, and federal law enforcement. Part I then contends that DHS—which does not share the same statutory data collection restraints as the FBI or NSA, for instance—may, in a matter of time, commandeer the real-time data flow from state and local law enforcement body-camera feeds and other live video feeds like from smart glasses if and when worn by law enforcement or other video feeds. This metadata, once collected, can be aggregated into databases that are open to interagency queries and information sharing amongst the entire intelligence community in such a manner that effectively renders moot much of the "post-Snowdengate"[26] legislative efforts meant to restrain such activity.

Part II provides a short overview of the NSA's metadata surveillance program as it was revealed by the Snowden disclosures.[27] This Part includes a brief discussion on how the metadata surveillance program was justified by the NSA under Section 215 of the USA PATRIOT Act and then subsequently challenged in U.S. federal courts following the Snowden disclosures. Part II sets forth an overview of the USA FREEDOM Act as a vehicle for resolving some of the disputes surrounding the legality and constitutionality of the NSA's metadata surveillance activities. It further summarizes why the USA FREEDOM Act is unlikely to bring metadata surveillance under proper oversight. These deficiencies include, for instance, the way in which the USA FREEDOM Act continues to allow for bulk metadata surveillance activities; the problem of "incidental" collection of the metadata of U.S. citizens during the course of foreign intelligence gathering; and the delegable nature of warrantless metadata surveillance that may allow for other intelligence agencies beyond the NSA to pursue bulk metadata collection of U.S. citizens under other authorities and contexts, such as the collection of data preserved by body cameras.

Part III asserts that the post-USA FREEDOM Act era awaits clarification from the Supreme Court on the contours of the protections that will be offered by the Fourth Amendment in the digital age. This Article concludes that any attempt to constrain bulk metadata surveillance will necessarily include an assessment of the efficacy of this surveillance method, as well as an evolution of the Fourth Amendment jurisprudence. Legislative reform alone that

26. *See generally* Margaret Hu, *Post-Snowdengate, Post-Fascism*, THEORETICAL INQUIRIES L. (forthcoming) (on file with the North Carolina Law Review) (discussing how, in a "post-fascist" world order built on laws and liberalism, technological advances by the NSA allowed it acquire massive amounts of information).

27. *See, e.g.*, Gellman et al., *supra* note 13.

focuses its attention on reining in the NSA's bulk telephony metadata collection program specifically and reining in the government's bulk collection of domestic records generally does not end the risk of mass metadata surveillance. The USA FREEDOM Act alone, therefore, is inadequate for its larger purpose: to secure freedom from mass surveillance and protection from suspicionless bulk metadata surveillance.

This Article concludes that rather than more tightly regulating bulk metadata collection, the Act allows for metadata surveillance to proceed under differing justifications and in more delegated contexts. The potential of ubiquitous body cameras presents a case study on why the USA FREEDOM Act is unable to effectively regulate bulk biometric metadata collection and other types of bulk metadata practices.

I. BODY CAMERAS AND BIOMETRIC DATA COLLECTION

Currently, body-worn cameras carried by state and local law enforcement are not ubiquitous nor are they multidimensional cybersurveillance systems.[28] Emerging multidimensional systems embrace "situational awareness" technologies that attempt to integrate multiple sensors such as video surveillance and other image sensors with web scraping of social media platforms.[29] Situational awareness technologies, for example, may aim to aggregate these surveillance methods with database screening and digital-watchlisting systems, such as DHS databases and the "No-Fly List," to assess risk.[30] Once pervasive, smart body cameras and smart glasses will

28. *See, e.g.*, *Body-Worn Camera Laws Database*, NAT'L CONF. ST. LEGISLATURES (Oct. 27, 2017), http://www.ncsl.org/research/civil-and-criminal-justice/body-worn-cameras-interactive-graphic.aspx [https://perma.cc/L38A-785C].

29. The integration of facial recognition technology with social media platforms and government databases yields significantly advanced surveillance capabilities in identifying and tracking individuals. Alessandro Acquisti, an associate professor of information technology and public policy at the Heinz College and a Carnegie Mellon CyLab researcher, for instance, conducted a series of experiments regarding social media sites and facial recognition. *See More than Facial Recognition*, CARNEGIE MELLON U., https://www.cmu.edu/homepage/society/2011/summer/facial-recognition.shtml [https://perma.cc/A9UH-YT97]. First, his team "identified individuals on a popular online dating site where members protect their privacy through pseudonyms." *Id.* Second, "they identified students walking on campus—based on their profile photos on Facebook." Third, they "predicted personal interests and, in some cases, even the Social Security numbers of the students, beginning only with a photo of their faces." *Id.*

30. *See, e.g.*, *DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy: Hearing Before the Subcomm. on Counterterrorism and Intelligence of the Comm. Of Homeland Sec.,* 112th Cong. 12–16 (joint statement of Mary Ellen Callahan, Chief Privacy Officer, Department of Homeland Security and Richard

likely work to collect biometric data and biometric metadata.[31] Biometric identification technologies—scanned fingerprints and irises, digitalized photos for facial recognition technology, and DNA, for example—increasingly inform law enforcement actions and support risk assessment tools. Once biometric identifiers are aggregated in databases, they can form the data backbone to support multidimensional cybersurveillance systems.

Body cameras, as a first-generation technology, are currently one-dimensional in their surveillance capacities (e.g., only collect video footage and audio).[32] As the technologies associated with body cameras evolve, they are likely to be used to tether biometric identity to multidimensional cybersurveillance (e.g., algorithmic-driven biographical screening and behavioral analysis).[33] Body cameras may also one day be deployed to assess future risk and to isolate other data deemed suspicious.[34]

A. What is Bulk Biometric Metadata Collection?

To explain why the USA FREEDOM Act is unlikely to accomplish its purported original objective of securing freedom from unwarranted and suspicionless mass surveillance,[35] bulk metadata

Chávez, Director, Office of Operations Coordination and Planning, Department of Homeland Security); *see also* ZYGMUNT BAUMAN & DAVID LYON, LIQUID SURVEILLANCE: A CONVERSATION 12 (2013); Margaret Hu, *Cybersurveillance Intrusions and an Evolving* Katz *Privacy Test*, 55 AM. CRIM. L. REV. 127, 133–37 (2018); Hu, *supra* note 6, at 1542–47; Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 64 (2014); Slobogin, *supra* note 23, at 1749–50.

31. *See, e.g.*, Alexandra Mateescu, Alex Rosenblat & danah boyd, Police Body-Worn Cameras 16–19 (Feb. 2015) (unpublished manuscript), https://www.datasociety.net/pubs/dcr/PoliceBodyWornCameras.pdf [https://perma.cc/QJF4-FBBS]; John Sanburn, *Storing Body Cam Data is the Next Big Challenge for Police*, TIME (Jan. 25, 2016), http://time.com/4180889/police-body-cameras-vievu-taser/ [https://perma.cc/DPH2-8SAP]; Jay Stanley, *Body Cameras Should Not Be Live-Streamed*, AM. CIV. LIBERTIES UNION: FREE FUTURE (Jan. 29, 2016), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/body-cameras-should-not-be-live-streamed [https://perma.cc/52H3-3XZR].

32. *See, e.g.*, *Research on Body-Worn Cameras and Law Enforcement*, NAT'L INST. JUST. (Dec. 5, 2017), https://www.nij.gov/topics/law-enforcement/technology/pages/body-worn-cameras.aspx [https://perma.cc/LY5D-6Z5Q].

33. *See, e.g.*, Margaret Hu, *Horizontal Cybersurveillance Through Sentiment Analysis*, 26 WM. & MARY BILL OF RTS. J. (forthcoming 2018) (manuscript at 5) (describing surveillance in the context of "sentiment analysis," a form of social media forecasting) (on file with the North Carolina Law Review).

34. Ava Kofman, *Taser Will Use Police Body Camera Videos "To Anticipate Criminal Activity"*, INTERCEPT (Apr. 30, 2017, 9:29 AM), https://theintercept.com/2017/04/30/taser-will-use-police-body-camera-videos-to-anticipate-criminal-activity/ [https://perma.cc/6Q4W-QUET].

35. *See* Andrea Peterson, *Why 76 Lawmakers Just Voted Against Their Own Bill to Reform the NSA*, WASH. POST (May 22, 2014), https://www.washingtonpost.com/news/the-

surveillance itself must be better understood. It is important to understand what metadata is, for instance, and why the intelligence community refers to metadata intelligence gathering and its accompanying search and analytic protocols as a "bulk metadata collection" and a "data query" program rather than a "surveillance" program.[36]

Metadata surveillance does not include the conversation of the call or the written text of the email.[37] Although digitalized surveillance methods are not new, automated and semi-automated bulk metadata surveillance methods are.[38] According to the NSA and

switch/wp/2014/05/22/why-76-lawmakers-just-voted-against-their-own-bill-to-reform-the-nsa/ [https://perma.cc/4LLB-S233] ("The Senate must take up the original USA FREEDOM Act—which clearly ends bulk collection and which includes more aggressive steps to protect Americans' privacy, such as important provisions to safeguard Americans from warrantless, backdoor searches of their private communications." (quoting statement of Sen. Mark Udall)); Valerie Plame, *Would You Rather Not Know?*, POLITICO MAG. (June 5, 2014), http://www.politico.com/magazine/story/2014/06/thanks-edward-snowden-107494 [https://perma.cc/XU9Z-GNEG] ("Our intelligence agencies should focus their efforts on terrorists and spies—and not law-abiding Americans." (quoting statement of Sen. Mark Udall)).

36. *See* Ewen MacAskill, *The NSA's Bulk Metadata Collection Authority Just Expired. What Now?*, GUARDIAN (Nov. 28, 2015, 8:00 AM), http://www.theguardian.com/us-news/2015/nov/28/nsa-bulk-metadata-collection-expires-usa-freedom-act [https://perma.cc/CC9P-T85G] ("The intelligence agencies hate the description 'mass surveillance' and insist what they are doing is bulk collection of data. They argue that although they gathered all this material, they only looked at a small part of it and, crucially, did not look at content."). *See generally* JENNIFER STISA GRANICK, AMERICAN SPIES: MODERN SURVEILLANCE, WHAT IT IS, & WHY YOU SHOULD CARE (2017) (describing the history of modern surveillance and the policy debate surrounding modern surveillance issues).

37. *See, e.g.*, Barton Gellman & Ashkan Soltani, *NSA Surveillance Program Reaches 'Into the Past' to Retrieve, Replay Phone Calls*, WASH. POST (Mar. 18, 2014), https://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html [https://perma.cc/YLP9-96MC] ("Most of the programs have involved the bulk collection of metadata—which does not include call content—or text, such as e-mail address books.").

38. Several scholars have noted how transformative technological shifts have also transformed methods of governance and surveillance as a tool of governance. *See, e.g.*, Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296, 2297 (2014) ("The digital era is different. Governments can target for control or surveillance many different aspects of the digital infrastructure that people use to communicate: telecommunications and broadband companies, web-hosting services, domain name registrars, search engines, social media platforms, payment systems, and advertisers."). *See generally* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1 (2008) (discussing the permanency and future of the national surveillance state); Jack M. Balkin & Sanford Levinson, *The Rehnquist Court and Beyond: Revolution, Counter-Revolution, or Mere Chastening of Constitutional Aspirations? The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 FORDHAM L. REV. 489 (2006) (describing the emerging regime of institutions and practices that make up the national surveillance state as the major constitutional

proponents of the bulk telephony metadata program, metadata collection is simply that: the collection or storage of pieces of metadata, data about data (e.g., time of a call).[39] Once databases are assembled (e.g., the time of the calls of Verizon subscribers on a specific date), NSA intelligence analyst is able to seek information by "querying" the database.[40]

From the Snowden disclosures, it appears the process of what we might call bulk biometric metadata collection may have already begun. Several NSA documents revealed that the NSA is compiling facial images extricated from intercepted communications via its global surveillance programs to be implemented in cutting-edge facial recognition initiatives.[41] The agency's utilization of facial recognition systems has expanded steadily—intercepting "millions of images per day" that include approximately 55,000 "facial recognition quality images."[42] The facial images represent "tremendous untapped potential," as the NSA explained in a 2011 document.[43] Therefore, this could be fairly characterized as a "bulk biometric collection" program. In other words, this disclosure appeared to reveal that the biometric data collection appears to be "bulk" (indiscriminate and suspicionless) and to share important similarities with the NSA's bulk telephony metadata collection program.

development of our era); David Lyon, *Biometrics, Identification and Surveillance*, 22 BIOETHICS 499 (2008) (describing emerging systems that automatically check biometric data); Erin Murphy, *Paradigms of Restraint*, 57 DUKE L.J. 1321 (2008) (describing the collection and use of biometric data to exercise control over individuals); Lior Jacob Strahilevitz, *Signaling Exhaustion and Perfect Exclusion*, 10 J. ON TELECOMM. & HIGH TECH. L. 321 (2012) (describing emerging biometric databases).

39. *See generally* Margo Schlanger, *Intelligence Legalism and the National Security Agency's Civil Liberties Gap*, 6 HARV. NAT'L SECURITIES J. 112 (2015) (arguing that the intelligence community focused on the legality of metadata collection rather than the policy rationale of the program); PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (2014), https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf [https://perma.cc/2R82-SFN3] (arguing that metadata is suggestive of the call's content and recommending that the telephone metadata collection program under Section 215 be discontinued).

40. *See, e.g.*, ACLU v. Clapper, 785 F.3d 787, 797 (2d Cir. 2015).

41. *See, e.g.*, James Risen & Laura Poitras, *N.S.A. Collecting Millions of Faces from Web Images*, N.Y. TIMES (May 31, 2014), https://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html [https://perma.cc/N73T-KLQX (dark archive)] (discussing Snowden disclosures that revealed that the NSA collects millions of digital photographs from Internet and social media sources and utilizes facial recognition technology to identify individuals).

42. *Id.*

43. *Id.*

To understand the similarities between what this Article refers to as NSA's bulk biometric collection program and NSA's bulk telephony metadata program, the rudimentary principles of facial recognition technology must be established. Facial recognition technology, like other biometric recognition technologies, necessitates a biometric template (e.g., face print from a digital photo).[44] Facial recognition technology is not dependent upon the actual digital photo, but rather, utilizes a method of transforming a face into a "vector of numbers which represent the facial image's characteristics including measurements [of facial features], color, lighting, 2D/3D [that facilitates] a Face Biometric Algorithm."[45] The process of algorithmically cross-referencing two facial images to determine a "match" is "not a match between two [biometric] templates, only a degree of statistical closeness."[46] Put differently, "algorithms are developed to 'match' the probability that the initial biometric data can be accurately compared to the currently presented biometric data or to make a determination that the data does not 'match.'"[47]

Because facial recognition entails an algorithmically-driven process, the NSA would not be focused on the content of the digital image itself. Rather, from this disclosure, it appears that the NSA is concerned about the data about the data (e.g., metadata and other data that can be gleaned from the facial image and digital photo or video image). Securing and examining the content of the photo does not appear to be the primary objective of the intelligence organization. Instead, from the disclosures and the NSA's response to this disclosure,[48] it appears the NSA is primarily interested in data analytics and metadata analysis that can be informed by bulk biometric collection, i.e, the facial coordinates or numerical information that can be pulled from the digital image intercepted

44. Hu, *supra* note 6, at 1534–35, 1534 n.349.

45. Marc Valliant, Vice President & Chief Tech. Officer, Animetrics, Face Recognition Technology Today, Presentation before the NTIA Multi-Stakeholder Process to Develop Consumer Data Privacy Code of Conduct Concerning Facial Recognition Technology (Feb. 25, 2014), https://www.ntia.doc.gov/files/ntia/publications/ntia_feb252014_marcvaillant.pdf [https://perma.cc/2EWZ-QVQW].

46. *Id.*

47. Hu, *supra* note 6, at 1535.

48. *See id.* (reporting that the Snowden documents stated "[i]t's not just traditional communications [the NSA is] after: It's . . . biographic and biometric information."); *see also* Joseph D. Moran, *NSA Metadata Collection and the Fourth Amendment*, 29 BERKELEY TECH. L.J. 985, 999 (2014) (noting that following the disclosures, both then-President Obama and then-Director of National Intelligence James Clapper emphasized the focus on metadata).

from the internet and social media, YouTube, Skype, etc.[49] In NSA documents from this disclosure, it is revealed that facial recognition technologies are integrated with a wide range of databases in order to build "comprehensive portraits of intelligence targets."[50]

Therefore, the Snowden disclosures surrounding bulk biometric collection may be viewed as programmatically parallel to the Snowden disclosures surrounding bulk telephony metadata collection. The bulk telephony metadata collection program revealed by the Snowden disclosures was not concerned with the content or the conversation of the call. This type of telephony metadata collection now falls within the regulation of the USA FREEDOM Act. Biometric metadata, specifically, could include photo and video metadata (e.g., time and place of image) and other biometric metadata (e.g., metadata from biometric templates and biometric information records).[51] Experts explain that a biometric template (e.g. face print, scanned fingerprint or iris), when combined with a name and biometric metadata, constitutes an "identifier" or a method to positively identify an individual or link an individual's identity to her biometric and biographic data.[52]

Bulk biometric collection and bulk biometric metadata collection operate similarly to the bulk telephony metadata program. Bulk biometric metadata collection programs are not necessarily concerned with the content or the substantive information revealed by the digital image. The Snowden disclosures revealed that the intelligence community was concerned with the analysis that could be associated with the metadata of telecommunications data. Similarly, the data and metadata aspects of the bulk biometric program appear to reveal that the intelligence community is concerned with the analysis that can be derived from facial recognition technology.[53] The bulk biometric and bulk biometric metadata collection programs are poised to increase exponentially with the normalization of body cameras, does not fall within the regulation of the USA FREEDOM Act.[54]

49. *See* Risen & Poitras, *supra* note 41 (discussing the NSA's use of metadata pulled from images stored on the internet).

50. *Id.*

51. *See, e.g.*, C. Tilton, *Biometric Authentication*, NAT'L INST. SCI. & TECH. (Dec. 13, 2016), https://www.nist.gov/sites/default/files/applyingmeasurementscienceworkshopjan12_13_2016.pdf [https://perma.cc/698U-JZKX].

52. Valliant, *supra* note 45.

53. *See e.g.*, Risen & Poitras, *supra* note 41.

54. After this disclosure, the NSA spokesperson explained that the collection of facial imagery was not justified under Section 215. *Id.* ("The N.S.A. does not collect facial imagery through its bulk metadata collection programs, including that involving

B. What is Bulk Biometric Metadata Used For?

To understand bulk biometric data, it is first important to understand more about biometrics. "Biometrics is generally understood to be "[t]he science of automatic identification or identity verification of individuals using [unique] physiological or behavioral characteristics."[55] To begin, biometric-based identification or identity verification systems can collect and analyze "hard biometrics," which is also known as "primary biometrics."[56] "Hard," or "primary," biometrics involve the traditional biometric identifiers that identity verification technologies use. These hard or primary biometrics can include "hand or finger images, facial characteristics, and iris recognition"[57] Government and industry alike use these biometric data systems to reach "secure identification and personal verification solutions."[58]

However, biometric-based identification, or identity verification, systems also can collect and analyze "soft biometrics."[59] Hard and soft biometrics can be distinguished based on how reliable the biometric identifier is perceived to be in automated identification matching technologies. Soft biometrics have been defined as "anatomical or behavioral characteristic[s] that provide[] some information about the identity of a person, but does not provide sufficient evidence to precisely determine the identity."[60] "Soft," or "secondary," biometric identification systems can employ digital analysis or automated determination of characteristics such as age, height, weight, race or ethnicity, skin and hair color, scars, birthmarks, and tattoos.[61] Behavioral characteristics also can be part of the identity verification and analysis. Behavioral biometric identifiers are explained as

Americans' domestic phone calls, authorized under Section 215 of the Patriot Act, according to Ms. [Vanee M.] Vines [the agency spokeswoman].").

55. JOHN R. VACCA, BIOMETRIC TECHNOLOGIES AND VERIFICATION SYSTEMS 589 (2007).

56. *See id.* at 590 (discussing "Biometric Technologies").

57. *See id.* at 3.

58. *Id.* at 57–59. Vacca does not provide a definitive definition of hard or primary biometric data. Nonetheless, he does offer background regarding biometric technology and verification system standards. Other scholars have explained that soft, or secondary, biometric characteristics have an experimental nature that can augment hard or primary biometric characteristics. *See e.g.*, Koichiro Niinuma, Unsang Park & Anil. K. Jain, *Soft Biometric Traits for Continuous User Authentication*, 5 IEEE TRANSACTIONS ON INFO. FORENSICS & SECURITY 771, 771–772 (2010).

59. *See, e.g.*, Niinuma et al, *supra* note 58 at 772 (defining the characteristics of both "soft" and "hard" biometrics).

60. Karthik Nandakumar & Anil K. Jain, *Soft Biometrics*, *in* ENCYCLOPEDIA OF BIOMETRICS 1235, 1235 (Stan Z. Li & Anil K. Jain eds., 2009).

61. *Id.*

"characteristics that are learned or acquired."[62] Examples of these identifiers are gait analysis—including the manner and pattern of walking—and voice identification.

After the collection of the biometric data, the data must be compiled in a database. This makes it possible to implement identity screening. When the government is the one to use these biometric identification technologies, it encourages surveillance, because biometric cybersurveillance not only identifies people, but also makes assessments based on identity. Biometric cybersurveillance thus constitutes an expansive inquiry; it surpasses determining who a person is to scrutinize people's intent, such as their criminal and terroristic dispositions. Furthermore, the identification might, but might not, involve traditional "surveillance" activities (e.g., domestic or foreign intelligence gathering). Consequently, progress in biometric identification and its widespread usages are transforming the nature of cybersurveillance.

Additionally, big data governance highlights how mass data collection and digitized assessments are being bureaucratized through practices that include data mining and database screening, digital watchlisting, algorithmic intelligence, and risk assessment and predictive analysis.[63] Increasingly, biometric data is incorporated into these technologies, anchoring the effect of cybersurveillance-dependent government programs.[64]

Presently, biometric data, when sourced specifically to be fed into verification and identification technologies, are generally regarded by the public and private spheres alike as benign.[65] Big data surveillance technologies allow for aggregating facial images with other databases and may constitute the first building block of a global photo database.

From the government's perspective, there is little distinction separating biometric credentialing as a reliable identification method from behavioral-biometric profiling as both initiatives share the same

62. VACCA, *supra* note 55, at 3.

63. *See* Margaret Hu, *Biometric Surveillance and Big Data Governance*, *in* CAMBRIDGE HANDBOOK ON SURVEILLANCE LAW 121 (David Gray & Stephen E. Henderson eds., 2017) (contending that "the biometric surveillance systems and precrime rationales fictionally portrayed in Steven Spielberg's film *Minority Report* are now emerging as a governance reality").

64. *See id.* (explaining how "[p]ublic and private decisionmaking protocols increasingly depend upon biometric identification technologies").

65. *See id.* at 126 (identifying the conception that "[b]iometric data is supposedly scientifically objective and utilize a purportedly neutral analysis of computer driven algorithmic analysis").

end goal: to advance security and pre-crime intervention via the combination of identification and risk analysis into one streamlined process.[66] Biometric data gathered for one use, however, is repurposed for another—something that is unavoidable in a big data world because the biometric cybersurveillance platforms are increasingly programmed to support mass-data compilation and predictive policing. This is particularly concerning from a privacy perspective when it comes to facial imagery derived from law enforcement body camera data feeds.

How biometric data can assist in targeting decisions, for example, has also been revealed through the Snowden disclosures and other revelations. Through recent media disclosures, it was reported that the Army has awarded at least a half-dozen contracts to technology firms to fuse facial recognition technology with drone technology.[67] Specifically, the contracts seek the development of algorithms that use two-dimensional images—like those that could be pulled from body camera feeds—to construct a 3D model of a face.[68] The software is becoming so advanced that other biometric data can be substituted for facial imagery, as Tim Faltemier, the lead biometrics researcher at Progeny Systems Corporation, explains:

> [I]f the system can't get a good enough look at a target's face, Progeny has other ways of IDing its prey . . . digital stereotyping using a series of so-called 'soft biometrics'—everything from age to gender to "ethnicity" to "skin color" to height and weight—the system can keep track of targets "at ranges that are impossible to do with facial recognition."[69]

The biometric data technology is not limited to surveillance in the small data sense—for example, watching an adversary. Through the pre-crime identification ambitions of big data, the defense contracts also reveal that the government aims to identify potentially hostile behaviors and uncover clandestine threats using a tool referred to as Adversary Behavior Acquisition, Collection,

66. *See id.* at 128 (detailing how in biometric cybersurveillance systems, "the inquiry expands from simply verification of identity . . . to include determination of identity . . . , as well as intent-related assessments").

67. Noah Shachtman, *Army Tracking Plan: Drones That Never Forget a Face*, WIRED (Sept. 28, 2011), https://www.wired.com/2011/09/drones-never-forget-a-face/ [https://perma.cc/2HVN-Z9UW].

68. *Id.*

69. *Id.*

Understanding, and Summarization ("ABACUS").[70] The technology would aggregate biometric data garnered from intercepted phone calls, social media and, potentially, body-camera footage and feed this information into a "human behavior modeling and simulation engine" that would generate "intent-based threat assessments of individuals and groups."[71] Put simply, ABACUS could potentially make a prediction as to which individuals are the most likely to commit acts of terrorism.

The qualitative distinction between this type of biometric data and the type of data derived from bulk telephony metadata collection as disclosed by Snowden is what makes technologies such as predictive policing so concerning from a privacy perspective. Whereas bulk telephony metadata collection programs return markers such as date, time, and location, facial recognition software platforms use images to identify certain points of an individual's facial symmetry and then discard the physical picture—retaining only the unique, identifying "map" of facial coordinates to be aggregated into a database.[72]

When migrated from foreign intelligence use or military use to domestic law enforcement uses, the current legislative and constitutional framework for regulating such technology appears to be absent.[73] Thus, the government may perceive that it is free to implement this technology in a legal vacuum. Similar to the lack of legal restraint on bulk telephony metadata collection prior to the Snowden disclosures, there is currently a lack of legal restraint on the scope and potential applications of bulk biometric data collection initiatives.[74]

70. *Id.*

71. *Id.*

72. *Id.*

73. *See, e.g.*, Margaret Hu, *Biometric Cyberintelligence and the Posse Comitatus Act*, 66 EMORY L.J. 697, 711–12 (2017).

74. *But see* Ted Claypoole & Cameron Stoll, *Developing Laws Address Flourishing Commercial Use of Biometric Information*, AM. BAR ASS'N (May 2016), https://www.americanbar.org/publications/blt/2016/05/08_claypoole.html [https://perma.cc/82XE-FDJE] (describing, inter alia, efforts by states—including Alaska, Arizona, California, Colorado, Idaho, Illinois, Florida, Kansas, Louisiana, Maine, Missouri, New Hampshire, North Carolina, Texas, West Virginia, Washington, and Wisconsin—to "regulate third parties' use and collection of individuals' biometric information"); *see, e.g.*, N.H. REV. STAT. ANN. § 260:10-b (West, Westlaw through Chapter 7 of the 2018 Reg. Sess.) (prohibiting collection of biometric data in connection with driver licensing).

C. Cooperative Biometric Data Sharing Between Privatized and State Law Enforcement and the Federal Government

Once biometric data (e.g., digital photo, scanned fingerprint. iris scan, or DNA) and biometric metadata (e.g., data associated with the biometric template) is collected and stored in bulk, bulk biometric metadata surveillance can be shared across entities—data can be shared between state and local law enforcement and the federal government; between the government and private contractors; and between civilian agencies and the intelligence and military communities.[75] For example, after the terrorist attacks of September 11, 2001, the U.S. Department of Justice ("DOJ"), the DHS, and other federal agencies encouraged cooperative data sharing as an effective counterterrorism tool.[76] Through programs such as Secure Communities, coordinated by DHS, state and local law enforcement organizations are required to share biometric data—digitally scanned fingerprints—with DHS.[77] Specifically, the biometric data is screened through DHS and FBI databases to determine if an arrestee is an undocumented immigrant and to facilitate digital watchlisting.[78]

Body cameras, once ubiquitous and multi-dimensional in their cybersurveillance capacities, can be used to facilitate cooperative data sharing between privatized law enforcement entities, state and local

75. *See* Claypoole & Stoll, *supra* note 74.

76. *See, e.g.*, Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735, 1778–92 (2015) (describing anti-terrorism programs that facilitate state and local law enforcement data sharing with federal government); Nathan Alexander Sales, *Mending Walls: Information Sharing After the USA PATRIOT Act*, 88 TEX. L. REV. 1795, 1797 (2010); Press Release, Transp. Sec. Admin., TSA to Test New Passenger Pre-Screening System (Aug. 26, 2004), http://www.tsa.gov/press/releases/2004/08/26/tsa-test-new-passenger-pre-screening-system [https://perma.cc/8RRW-8L9P] (announcing the "Secure Flight" program, a post-9/11 prescreening program that compares passenger lists with terrorist watchlists to assist in maintaining "no fly" lists).

77. *See, e.g.*, Adam B. Cox & Thomas J. Miles, *Policing Immigration*, 80 U. CHI. L. REV. 87, 110–34 (2013); Christopher N. Lasch, *Rendition Resistance*, 92 N.C. L. REV. 149, 209–16 (2013); Thomas J. Miles & Adam B. Cox, *Does Immigration Enforcement Reduce Crime? Evidence from Secure Communities*, 57 J. L. & ECON. 937, 938–39 (2014).

78. DHS explains that Secured Communities is justified by a combination of authorities. *See* Memorandum from Riah Ramlogan, Deputy Principal Legal Advisor, to Beth N. Gibson, Assistant Deputy Dir., U.S. Dep't of Homeland Sec., U.S. Immigration & Customs Enforcement 1 (Oct. 2, 2010), http://uncoverthetruth.org/wp-content/uploads/2012/01/Mandatory-in-2013-Memo.pdf [https://perma.cc/P4DU-B5A6]. DHS relied upon the following: (1) 28 U.S.C. § 534(a)(1) (2012) and 28 U.S.C. § 534(a)(4) together provide the FBI with authority to share fingerprint data with ICE/DHS; (2) 8 U.S.C. § 1722 mandates the development of a data sharing system that "enable(s) intelligence and law enforcement agencies to determine the inadmissibility or deportability of an [undocumented immigrant]"; and (3) 42 U.S.C. § 14616 ratifies information or database sharing between federal and state agencies. *Id.* at 4–6.

law enforcement, and the federal government. Secure Communities provides a concrete example of how the data collected by state and local law enforcement through body cameras may one day be placed into the service of federal database screening and digital watchlisting systems. Additionally, the bulk biometric collection program revealed by the Snowden disclosures indicated that in one NSA PowerPoint slide, a facial image of "an unidentified man" included "more than two dozen data points" that included "whether he was on the Transportation Security Administration no-fly list, his passport and visa status, known associates or suspected terrorist ties, and comments made about him by informants."[79]

Reporting on surveillance practices has helped to reveal domestic law enforcement's ever-increasing ability to use biometric surveillance, thanks to multi-dimensional cybersurveillance tools. For example, media reports have revealed that state and local enforcement have partnered with corporations to experiment with biometric surveillance that relies upon live-feed video surveillance and real-time social media screening.[80] In some instances the law enforcement agency solicits a corporate surveillance product and in other instances the corporation may solicit a collaboration with the state or local law enforcement organization.[81] In one program, for example, a corporation tested a Smart Surveillance System and Intelligent Video Analytics software with cooperation with a city to conduct surveillance of a concert.[82] The program assimilated and aggregated information on live video and social media activity through monitoring of crowds, pedestrians, and vehicles.[83] The "situational awareness software" was defined as

79. Risen & Poitras, *supra* note 41.

80. *See* Luke O'Neil, *Beantown's Big Brother: How Boston Police Used Facial Recognition Technology to Spy on Thousands of Music Festival Attendees*, NOISEY (Aug. 13, 2014, 12:00PM), https://noisey.vice.com/en_us/article/beantowns-big-brother [https://perma.cc/DXB6-WKY7].

81. In one media disclosure, for example, it was revealed that IBM and the city of Boston had collaborated on a situational awareness system since March of 2012, when IBM gave Boston a grant through its "Smarter Cities Challenge." Chris Faraone, Kenneth Lipp & Jonathan Riley, *Boston Trolling (Part 2)*, DIGBOSTON (Oct. 9, 2014), https://digboston.com/boston-trolling-part-2/#sthash.fdmnpZxN.dpbs [https://perma.cc/LH3C-FG6X].

82. Chris Faraone, Kenneth Lipp & Jonathan Riley, *Boston Trolling (Part I): You Partied Hard at Boston Calling and There's Facial Recognition Data to Prove It*, DIGBOSTON (Aug. 7, 2014), https://web.archive.org/web/20140924133220/https://digboston.com/boston-news-opinions/2014/08/boston-trolling-part-i-you-partied-hard-at-boston-calling-and-theres-facial-recognition-data-to-prove-it/ [https://perma.cc/4NHM-8SFM].

83. *Id.*

> software [that] analyzes video and provides alerts when something happens. For example, if someone walks into a secure area in view of one of the system's cameras, the software would raise a red flag. More sophisticated systems can track people in real time as they move through crowds — such as following an unauthorized person in the area — without requiring dozens or even hundreds of human analysts to watch video feeds.[84]

In practice, the situational awareness tool integrated live social media tracking into already-installed city cameras to screen individuals for biometric tracking and "forensic identification purposes."[85] Notably, the surveillance had a "People Search" feature that could identify individuals by skin color, clothing texture, baldness, or whether or not they wear glasses.[86] Although the program claimed that there was no use of the facial capture and facial recognition technology,[87] the program possessed the capacity to conduct such tracking.[88] These situational awareness programs show the significant increase in the real time technological capabilities of using biometric capture and recognition software. However, the programs remain highly experimental, with their efficacy and accuracy unknown.[89]

Consequently, these technologically evolving surveillance programs are not necessarily carried out by traditional law enforcement. Rather, state and local law enforcement are increasingly relying upon corporate and federal situational-awareness surveillance products. Multidimensional cybersurveillance tools are expanding in their purported capacities to assess risk. With evolving technologies, like body cameras, state and local officers could receive real-time alerts and information from corporate and federal surveillance products that may scrape social media, for instance, permitting the

84. Nestor Ramos, *City Used High-Tech Tracking Software at '13 Boston Calling*, BOS. GLOBE (Sept. 8, 2014), https://www.bostonglobe.com/metro/2014/09/07/boston-watching-city-acknowledges-surveillance-tests-during-festivals/Sz9QVurQ5VnA4a6Btds8xH/story.html [https://perma.cc/4CXY-EPDX].

85. Faraone et al., *supra* note 81.

86. *Id.*

87. *Id.* (noting that despite those claims, photographs from the IOC obtained and published by reporters appeared to show Boston Police Officers present during the IOC test during the event).

88. Ramos, *supra* note 84.

89. *See* Tim De Chant, *The Limits of Facial Recognition*, NOVANEXT (Apr. 26, 2013), http://www.pbs.org/wgbh/nova/next/tech/the-limits-of-facial-recognition/ [https://perma.cc/QXM9-XWU4].

officers to respond to ongoing situations.[90] Body-camera technology could one day allow law enforcement to sort through social media photos with facial recognition technology to compile biometric and biographic profiles of anyone who presents their face in public, for instance, in a crowd or in a vehicle.[91]

Data generated by ubiquitous body cameras could be captured and monetized by corporations as pre-crime intervention products. The dual purpose and symbiotic relationship of body-camera surveillance and corporate data surveillance might operate in the following manner: Law enforcement investigative and monitoring techniques could be converted into more accurate consumer monitoring, and the consumer monitoring and trend tracking could have the potential to be exploited for law enforcement investigation. Therefore, these growing capacities to conduct situational-awareness surveillance or multi-dimensional cybersurveillance show how law enforcement, homeland security, and intelligence and military communities could use body-camera data and corporate-delegated surveillance to engage in comprehensive monitoring and biometric-behavioral profiling.

II. BULK TELEPHONY METADATA COLLECTION

As the following discussion in Parts II and III illuminates, the statutory framework necessary to regulate data sharing, both within the intelligence community writ large and between federal and state and local law enforcement, is lacking. The degradation of federalism in the law enforcement context will likely exacerbate the legal challenges associated with the large-scale installation of police body cameras. As body-camera data becomes more available, the federal government, particularly DHS, may attempt to commandeer the real-

90. *See* Andy Cush, *Social Media Surveillance Probably Played a Role in Sparking the Freddie Gray Riot*, SPIN (Oct. 14, 2016), https://www.spin.com/2016/10/social-media-surveillance-probably-played-a-role-in-sparking-the-freddie-gray-riot/ [https://perma.cc/MEF8-CAQG] (explaining how Geofeedia monitored protests and alerted Baltimore officers to high school students who "planned to walk out of class and use mass transit to head to the Mondawmin Mall protests," allowing officers to intercept the students before they arrived at a protest).

91. *Id.*; *see, e.g.*, Romine Testimony, *supra* note 7, at 21 ("The latest FRVT [NIST Face Recognition Vendor Testing Program] (launched July 2012) evaluated large-scale one-to-many face recognition algorithms from still face photos and (for the first time) from video, along with testing automated methods for detecting pose, expression, and gender."); Brian Shockley, *Vigilant Solutions Unveils Mobile Companion App at IACP*, VIGILANT SOLUTIONS (Oct. 23, 2014), https://www.vigilantsolutions.com/stories-from-the-street/vigilant-mobile-companion-app-iacp [https://perma.cc/2Z6P-PCU9] (describing systems that combine facial recognition technology with automated license plate readers).

time biometric data stream from local law enforcement. Once DHS and other federal agencies, including intelligence and military organizations, gain unfettered access to an exponentially larger amount of body-camera data, such data can then be compiled into databases to be aggregated, shared, and applied to a wide range of pre-crime surveillance uses.

The Snowden disclosures suggest that metadata collection and database queries of stored metadata are not characterized as surveillance activities by the NSA.[92] The bulk telephony metadata program revealed by the Snowden disclosures did not include an analysis of "content"—i.e., an examination of the conversation or review of the substantive information shared in the phone call—because this distinction was legally significant to the intelligence community and the Foreign Intelligence Surveillance Court ("FISC") in distinguishing between a "collection" program and a "surveillance" program.[93] The Snowden disclosures, importantly, revealed that by discounting the surveillance implications of bulk metadata collection and database queries, the intelligence community argued, and the FISC agreed, that Fourth Amendment protections were inapplicable to metadata surveillance.[94]

Properly regulating bulk metadata collection by the NSA thus is complicated significantly by the fact that bulk metadata surveillance technically does not fall within the category of "content"

92. Because Section 215 of the USA PATRIOT Act allows for the collection of business records, it appears that the bulk telephony metadata program was characterized by the government as a business records collection program, not as a metadata surveillance program. Pub. L. No. 107-56, sec. 215, § 501, 115 Stat. 272, 287–88 (2001) (codified as amended at 50 U.S.C. § 1861 (2012))*; see, e.g.*, Klayman v. Obama, 957 F. Supp. 2d 1, 14 (D.D.C. 2013) ("In broad overview, the Government has developed a 'counterterrorism program' under [Section 215 of the USA PATRIOT Act, codified in the U.S. Code at] Section 1861 in which it collect[s], compiles, retains, and analyzes certain telephone records, which it characterizes as 'business records' created by certain telecommunications companies (the 'Bulk Telephony Metadata Program'). The records collected under this program consist of 'metadata,' such as information about what phone numbers were used to make and receive calls, when the calls took place, and how long the calls lasted." (citations omitted)), *rev'd on other grounds*, 800 F.3d 559 (D.C. Cir. 2015); *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted], No. BR 06-05, 2006 U.S. Dist. LEXIS 101368, at *2 (FISA Ct. May 24, 2006) (describing information collected as "session identifying information," including "trunk identifier" and "time and duration of call.").

93. *See* MacAskill, *supra* note 36. *See generally* GRANICK, *supra* note 36 (detailing the history of the policy and legal debate on modern surveillance and arguing that modern surveillance and democracy are incompatible).

94. *See* MacAskill, *supra* note 36.

surveillance.[95] Historically, the intelligence community utilized traditional surveillance methods to probe the content of the communication intercepted—for instance, the content of a phone call (e.g., the conversation) or the content of a written correspondence (e.g., text of the letter, telegram, or an email).[96] Traditional small data intelligence gathering methods have relied upon human intelligence, including: sensory perception analysis and other communication gathering and analytic methods that depended upon human judgment and decision-making; traditional evidence based upon analog data and paper-based files; conventional intelligence collection methods, such as traditional signals intelligence and other traditional communications interception; and other data analytic tools that have centered upon traditional research approaches, such as hypothesis-driven methods.[97]

95. *See Klayman*, 957 F. Supp. 2d at 15 ("According to the representations made by the Government, the metadata records collected under the program do *not* include *any* information about the content of those calls, or the names, addresses, or financial information of any party to the calls. Through targeted computerized searches of those metadata records, the NSA tries to discern connections between terrorist organizations and previously unknown terrorist operatives located in the United States." (footnote and citations omitted)); *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted], 2006 U.S. Dist. LEXIS 101368, at *2 ("Telephony metadata does not include the substantive content of any communication . . . , or the name, address, or financial information of a subscriber or customer.").

96. *See generally* ROBERT M. CLARK, INTELLIGENCE COLLECTION (2014) (explaining methods of intercepting phone calls and written correspondence); ROBERT WALLACE, H. KEITH MELTON, & HENRY R. SCHLESINGER, SPYCRAFT: THE SECRET HISTORY OF THE CIA'S SPYTECHS, FROM COMMUNISM TO AL-QAEDA (2008) (recounting the history of the CIA and explaining methods used by the agency to conduct intelligence operations). Multiple scholars have discussed the Fourth Amendment implications of rapidly evolving technologies. *See, e.g.*, STEPHEN J. SCHULHOFER, MORE ESSENTIAL THAN EVER: THE FOURTH AMENDMENT IN THE TWENTY-FIRST CENTURY 115–43 (2012); David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381, 385–91 (2013); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313–14 (2012); Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 481–82 (2011); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution,* 102 MICH. L. REV. 801, 802–05 (2004); Benjamin Wittes, *Databuse: Digital Privacy and the Mosaic*, BROOKINGS INST. JUST. (Apr. 1, 2011), http://www.brookings.edu/research/papers/2011/04/01-databuse-wittes [https://perma.cc/4988-KSA3]. Other scholars have explained necessary statutory reforms needed to keep pace with these technological developments. *See, e.g.*, Donohue, *Bulk Metadata Collection*, *supra* note 23, at 900; Donohue, *Section 702*, *supra* note 23, at 265; Margulies, *supra* note 23, at 5; Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1, 17–34 (2012).

97. *See* Faraone et al., *supra* note 81.

Because metadata collection technically does not include content—for example, collection of metadata includes the time of call and location of call, but does not include eavesdropping on the conversation—the privacy concerns associated with its collection are often underestimated.[98] For instance, shortly after the Snowden disclosures, Senator Dianne Feinstein, then Chair of the Senate Intelligence Committee, explained that metadata collection is not surveillance in that it is pure "content-less" data.[99] In contrast, Bruce Schneier, a renowned cybersecurity expert, has stated unequivocally that bulk metadata collection is coterminous with modern surveillance—an equivalency that potentially implicates significant privacy concerns.[100]

Consequently, even with passage of the USA FREEDOM Act, metadata surveillance by the intelligence community is significantly under-regulated.[101] At the dawn of the big data revolution, the U.S. political branches and U.S. federal courts appear to be conflicted about how to treat metadata collection under preexisting intelligence governance structures and the U.S. Constitution.[102] Some have argued

98. *See* ACLU v. Clapper, 785 F.3d 787, 794 (2d Cir. 2015) ("That telephone metadata do not directly reveal the content of telephone calls . . . does not vitiate the privacy concerns arising out of the government's bulk collection of such data.").

99. Ed O'Keefe, *Transcript: Dianne Feinstein, Saxby Chambliss Explain, Defend NSA Phone Records Program*, WASH. POST (June 6, 2013), http://www.washingtonpost.com/news/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program/ [https://perma.cc/2HYJ-RMKF]. Senator Feinstein defended the NSA bulk telephony metadata collection program in the following way: "[T]his is just metadata. There is no content involved." *Id*.

100. Bruce Schneier, *Metadata = Surveillance*, SCHNEIER ON SECURITY (Mar. 13, 2014, 12:13 PM), https://www.schneier.com/blog/archives/2014/03/metadata_survei.html [https://perma.cc/AP3T-NSQ2] ("Metadata equals surveillance data, and collecting metadata on people means putting them under surveillance.").

101. *See* David Cole, *Here's What's Wrong with the USA FREEDOM Act*, NATION (May 6, 2015), http://www.thenation.com/article/heres-whats-wrong-usa-freedom-act/ [https://perma.cc/6XPR-963Y]; Dan Froomkin, *USA FREEDOM Act: Small Step for Post-Snowden Reform, Giant Leap for Congress*, INTERCEPT (June 2, 2015, 6:08 PM), https://theintercept.com/2015/06/02/one-small-step-toward-post-snowden-surveillance-reform-one-giant-step-congress/ [https://perma.cc/RZD4-4FW6]; *see also* Banks, *supra* note 23, at 1636; Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 951, 954 (2006).

102. The bulk telephony metadata collection program, as had been legally justified under Section 215 of the USA PATRIOT Act, faced multiple legal challenges under several legal theories, with lawsuits filed in federal court immediately following the June 5, 2013 Snowden disclosures. *See, e.g.*, Klayman v. Obama, 142 F. Supp. 3d 172, 182–195 (D.D.C. 2015) (concluding that plaintiff's claim that Section 215 program is unconstitutional under the Fourth Amendment has a likelihood of success on the merits and ordering injunction, blocking the final weeks of the Section 215 program prior to the implementation of the USA FREEDOM Act's reforms to metadata collection), *stay granted sub nom*, Obama v. Klayman, 1:13-cv-00851-RJL, 2015 WL 9010330 (D.C. Cir.

that metadata collection should not fall within traditional conceptions of what is considered surveillance and, therefore, should not be regulated in the same manner as traditional surveillance methods.[103]

Some in the government have explicitly drawn a distinction between content and non-content surveillance to explain how the latter falls outside the scope of many of the legal restrictions and other regulatory constraints imposed on the surveillance activities of the intelligence community.[104] In contrast, some contend that the pervasive, comprehensive, and automated or semi-automated nature of bulk metadata surveillance leads to greater harms than the types of harms enabled by traditional content surveillance.[105] Experts, for

Nov. 16, 2015), *petition for rehearing en banc denied*, 805 F.3d 1148 (D.C. Cir. 2015) (mem.); Klayman v. Obama, 957 F. Supp. 2d 1, 19, 30 (D.D.C. 2013) (finding court lacked jurisdiction to review Administrative Procedures Act [APA] claim but could hear Fourth Amendment constitutional challenges to NSA's conduct; and granting motion for injunction, however, staying the order pending appeal), *rev'd sub nom and remanded*, Obama v. Klayman, 800 F.3d. 559, 561 (D.C. Cir. 2015); *see also* ACLU v. Clapper, 959 F. Supp. 2d 724, 757 (S.D.N.Y. 2013) (dismissing complaint in part on grounds that subscribers do not have legitimate expectation of privacy in telephony metadata held by third parties under Fourth Amendment), *vacated*, 785 F.3d. 787, 792 (2d Cir. 2015) (finding that bulk collection of telephone metadata exceeded scope of statutory authority, remanding for argument on constitutional issues, and affirming district court's denial of preliminary injunction), *stay ordered*, 2015 WL 4196833 (2d Cir. June 9, 2015) (ordering stay of proceedings pending parties' supplemental briefing in light of passage of USA FREEDOM Act), *remanded*, 804 F.3d 617 (2d Cir. 2015) (denying motion for preliminary injunction, declining to reach constitutional issues for prudential reasons); Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 44 PEPP. L. REV. 773, 809–10 (2015).

103. *See, e.g.*, O'Keefe, *supra* note 99 (statements of Sens. Dianne Feinstein and Saxby Chambliss).

104. *See In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted], No. BR 13-109, 2013 WL 5741573, at *5 n.18 (FISA Ct. Aug. 29, 2013) ("In *In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d)*, the court found that only the service provider, as opposed to a customer or subscriber, could challenge the execution of a § 2703(d) non-content records order. The court reasoned that '[b]ecause Congress clearly provided . . . protections for one type of § 2703 order [content] but not for others, the Court must infer that Congress deliberately declined to permit challenges for the omitted orders.' The court also noted that the distinction between content and non-content demonstrates an incorporation of *Smith v. Maryland* into the SCA. As discussed above, the operation of Section 215 within FISA represents that same distinction." (alterations in original) (citations omitted) (quoting *In re* Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 128 (E.D. Va. 2011))).

105. *See, e.g.*, *Clapper*, 785 F.3d at 794 ("[A] call to a single-purpose telephone number such as a "hotline" might reveal that an individual is: a victim of domestic violence or rape; a veteran; suffering from an addiction of one type or another; contemplating suicide; or reporting a crime. Metadata can reveal civil, political, or religious affiliations; they can also reveal an individual's social status, or whether and when he or she is involved in intimate relationships. . . . The more metadata the government collects and analyzes, . . . the greater the capacity for such metadata to reveal ever more private and previously

example, have explained that metadata collection is and should be regulated as a new form of surveillance in that it is even more intrusive than traditional intelligence-gathering methods and can reveal a "startling amount of detailed information"[106] in the aggregate that content surveillance standing alone is incapable of revealing.

Grasping the legal and technological distinctions between "content" surveillance and "non-content" surveillance in the eyes of the intelligence community and the FISC underscores why metadata surveillance appears to be justified by those within the NSA and the intelligence community. The USA FREEDOM Act does not resolve the tension between "content" surveillance and "non-content" surveillance. Therefore, even after passage of the USA FREEDOM Act, there is still an open debate regarding whether "non-content" surveillance such as bulk metadata surveillance should fall within the same oversight and accountability mechanisms that constrain "content" surveillance. Without a resolution of this tension, bulk metadata surveillance is likely to continue without proper oversight and constraint.

A. The NSA's Bulk Telephony Metadata Collection Program Under Section 215 of the USA PATRIOT Act

Much of what we know about the NSA's bulk metadata collection program stems from documents released through the Snowden disclosures.[107] In June 2013, the disclosures by former NSA contractor Edward Snowden revealed that the U.S. intelligence organization had collected the bulk telephony metadata on every call generated by customers of the multinational telecommunications company, Verizon, on a daily basis over the course of the past seven years.[108] Approved through a classified order by the FISC, the bulk metadata collected by the NSA included the time of the call and the

unascertainable information about individuals."); *see also* Declaration of Professor Edward W. Felten at 20, *Clapper*, 959 F. Supp. 2d 724 (No. 13 Civ. 3994(WHP)) ("Metadata analysis can reveal the rise and fall of intimate relationships, the diagnosis of a life-threatening disease, the telltale signs of a corporate merger or acquisition, the identity of a prospective government whistleblower, the social dynamics of a group of associates, or even the name of an anonymous litigant.").

106. *Clapper*, 785 F.3d at 794.

107. The Snowden disclosures were first revealed by journalist Glenn Greenwald in June 2013. For an extensive historical account of the Snowden disclosures, see generally GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE (2014).

108. *See* Greenwald, *supra* note 17.

length of the call.[109] The NSA's bulk telephony metadata collection program also included: comprehensive communications routing information; the international mobile subscriber identity number; the trunk identifier; telephone calling card numbers; and other metadata.[110] Whether the geolocation of the call was included in this bulk collection program is disputed.[111]

In the litigation that followed the Snowden disclosures, it remains judicially unresolved whether metadata collection is either statutorily or constitutionally permissible.[112] Further complicating the adjudication of these matters, the FISC had adopted the NSA's view and held in 2006 that the prior bulk telephony metadata collection program was justified under Section 215 of the USA PATRIOT Act.[113] In the post-Snowden litigation, federal courts have grappled

109. *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted], No. BR 06-05, 2006 U.S. Dist. LEXIS 101368, at *1–2 (FISA Ct. May 24, 2006) ("[Here] 'telephony metadata' includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call."); *see also* Greenwald, *supra* note 17.

110. *See* Amici Curiae Brief of Experts in Computer and Data Science in Support of Appellants and Reversal at 7, *Clapper*, 785 F.3d 787 (No. 14-42) (citing *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted], 2013 WL 5741573, at *1 n.2 (FISA Ct. Aug. 29, 2013)).

111. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 15 n.17 (D.D.C. 2013) ("Plaintiffs have alleged that the Government has collected location information for cell phones. While more recent FISC opinions expressly state that cell-site location information is not covered by Section 1861 production orders, the Government has not affirmatively represented to this Court that the NSA has not, at any point in the history of the Bulk Telephony Metadata Program, collected location information (in one technical format or another) about cell phones." (citations omitted)), *rev'd on other grounds*, 800 F.3d 559 (D.C. Cir. 2015); *see also* Amici Curiae Brief of Experts in Computer and Data Science in Support of Appellants and Reversal, *supra* note 110, at 7 (claiming that a trunk identifier provides "revealing general information about [a] part[y's] location").

112. *See e.g.*, *Clapper*, 785 F.3d at 792 (2d Cir. 2015) (finding that "the program exceed[ed] the scope of what Congress has authorized" under the USA PATRIOT Act); *Obama,* 800 F.3d. at 568 (D.C. Cir. 2015) (finding "that plaintiffs have failed to demonstrate a 'substantial likelihood' that the government is collecting from Verizon Wireless or that they are otherwise suffering any cognizable injury"). *Compare Klayman*, 957 F. Supp. 2d at 41 (holding that, for purposes of injunctive relief, plaintiff subscribers had "a substantial likelihood of showing that . . . the NSA's bulk collection program is indeed an unreasonable search under the Fourth Amendment"), *with* United States v. Moalin, No. 10cr4246 JM, 2013 WL 6079518, at *5 (S.D. Cal. Nov. 18, 2013) (holding that there is no reasonable expectation of privacy in telephony metadata under the Fourth Amendment), *and In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted]*, 2013 WL 5741573, at *2–3 (same).

113. *See, e.g.*, *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted]*, 2013 WL 5741573, at *4–6; *see also In re Application of the FBI*

with the question of whether bulk telephony metadata could be permissibly construed under the statute as a "tangible" business record "relevant to any particular investigation," as had been the government's interpretation of Section 215.[114]

According to the government, the statutory basis for bulk telephony metadata collection expressly derives from Section 215 of the USA PATRIOT Act, which authorizes the following collection: "any tangible things (including books, records, papers, documents, and other items)."[115] Under the USA PATRIOT Act, "the Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things."[116] These "tangible things," however, must be "relevant to an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[117] Snowden's disclosures revealed that the government had successfully argued in the FISC that bulk collection of data was necessary ex ante under Section 215 of the USA PATRIOT Act.[118] The U.S. Court of Appeals for the D.C. Circuit found that the district court had erred in granting a preliminary injunction barring the government from collecting bulk telephony metadata under Section 215 of the Act because any lapse in bulk collection was temporary where the FISC viewed the Act as effectively reinstating Section 215 for 180 days and allowing it to resume issuing bulk collection orders during that window.[119] The bulk telephony metadata program provides the government with an aggregate of data (e.g., metadata on all phone calls collected from Verizon on a daily basis, which allows the NSA to collect the "phone records of millions of Verizon customers daily").[120] Once the bulk

for an Order Requiring the Prod. of Tangible Things from [Redacted], 2006 U.S. Dist. LEXIS 101368, at *3 (granting the NSA's application to collect bulk telephony metadata).

114. *See, e.g.*, *Clapper*, 785 F.3d at 810–11.

115. USA PATRIOT Act of 2001, Pub. L. No. 107-56, sec. 215, § 501(a)(1), 115 Stat. 272, 287 (codified as amended at 50 U.S.C. § 1861(a)(1) (2012)).

116. *Id.*

117. 50 U.S.C. § 1861(b)(2)(A) (2012).

118. *See, e.g.*, Klayman v. Obama, 957 F. Supp. 2d 1, 10 (D.D.C. 2013), *rev'd on other grounds*, 800 F.3d 559 (D.C. Cir. 2015); *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from Verizon Bus. Network Servs., Inc., No. BR 13-80, at 1–2 (FISA Ct. Apr. 25, 2013), https://epic.org/privacy/nsa/Section-215-Order-to-Verizon.pdf [https://perma.cc/7KB6-FX45].

119. Obama v. Klayman, 800 F.3d. 559, 561–62 (D.C. Cir. 2015).

120. Greenwald, *supra* note 17.

data is amassed, the NSA may query a specific identifier within the aggregated database and determine the relevance of the data to an ongoing investigation.[121]

In challenges filed immediately after the Snowden disclosures, federal courts attempted to resolve whether the NSA's bulk telephony metadata collection program was consistent with constitutional protections such as the First Amendment's associational and expressive freedom guarantees, and the Fourth Amendment's proscription against unreasonable searches and seizures.[122] The issue of whether the Act constitutionally resolves metadata surveillance remains unclear.[123] As discussed below, federal courts in the post-Snowden litigation appear reluctant to reach the question of whether bulk telephony metadata collection is constitutional under the First Amendment and the Fourth Amendment.[124]

121. "After collecting these telephone records, the NSA stores them in a centralized database. Initially, NSA analysts are permitted to access the Section 215 calling records only through 'queries' of the database. A query is a search for a specific number or other selection term within the database." PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., *supra* note 39, at 8; *see also Klayman*, 957 F. Supp. 2d at 15 ("According to Government officials, this aggregation of records into a single database creates 'an historical repository that permits retrospective analysis,' Govt.'s Opp'n at 12, enabling NSA analysts to draw connections, across telecommunications service providers, between numbers reasonably suspected to be associated with terrorist activity and with other, unknown numbers."); *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted], No. BR 13-109, 2013 WL 5741573, at *6–7 (FISA Ct. Aug. 29, 2013); Christopher Slobogin, *Cause To Believe What? The Importance of Defining a Search's Object—Or, How the ABA Would Analyze the NSA Metadata Surveillance Program*, 66 OKLA. L. REV. 725, 737 (2014) ("But at the time of the bulk collection, those links would not be known; the NSA would subsequently have to query the data to learn about those links. Thus, one would be hard pressed to say that, at the time of the bulk collection, the government meets the relevance standard, much less the probable cause or reasonable suspicion standards, if the object of the seizure is *Redding*'s [Safford Unified School District #1 v. Redding, 557 U.S. 364, 370 (2009)] 'evidence of criminal activity' or the LEATPR [American Bar Association's Criminal Justice Standards on Law Enforcement Access to Third Party Records] Standards 'evidence of crime' that is associated with the probable cause and reasonable suspicion standards.").

122. *See, e.g.*, Klayman v. Obama, 142 F. Supp. 3d 172, 183, 189 (D.D.C. 2015) (finding that plaintiffs had demonstrated a substantial likelihood of success on Fourth Amendment claim collection and querying of bulk telephony metadata records constituted an unconstitutional search).

123. *See id.* at 178 (granting preliminary injunction to enjoin "the future collection and querying of [plaintiffs'] telephone record metadata" on basis that Section 215 program is unconstitutional); *vacated by* Klayman v. Obama, 805 F.3d 1148, 1148 (D.C. Cir. 2015); Motion to Vacate Preliminary Injunction and Dismiss Appeal on Grounds of Mootness, Klayman v. Obama, 15-5307 (D.C. Cir. Jan. 4, 2016) (filing motion to dismiss matter as moot in light of enactment and implementation of USA FREEDOM Act).

124. *See infra* Section II.B.

B. Post-Snowden Legislative Reform: The USA FREEDOM Act

The most developed litigation challenging the legality and constitutionality of the NSA's bulk telephony metadata collection program is represented by two cases: *ACLU v. Clapper*[125] and *Klayman v. Obama*.[126] Both of these challenges to the Section 215 bulk metadata collection program in federal court were brought days after the Snowden disclosures first came to light in June 2013.[127] U.S. District Court Judge William H. Pauley III for the Southern District of New York, in *ACLU v. Clapper*, and U.S. District Court Judge Richard Leon for the District of Columbia, in *Klayman v. Obama*, considered the same program—NSA's bulk telephony metadata collection program—and reached entirely different results in their considerations of injunctive relief for their plaintiffs.[128] In both *Clapper* and *Klayman*, the plaintiffs asserted a combination of statutory and constitutional claims[129] to challenge the bulk telephony metadata program that derived from a April 25, 2013 FISC order compelling Verizon Business Network Services to produce to the NSA on "an ongoing daily basis . . . all call detail records or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls," pursuant to Section 215 of the USA PATRIOT Act.[130]

125. 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (dismissing complaint in part on grounds that subscribers do not have legitimate expectation of privacy in telephony metadata held by third parties under Fourth Amendment precedent), *vacated*, 785 F.3d. 787 (2d Cir. 2015).

126. 957 F. Supp. 2d 1, 9 (D.D.C. 2013) (finding that court lacked jurisdiction to review Administrative Procedure Act ["APA"] claim but could hear Fourth Amendment constitutional challenges to NSA's conduct, and granting motion for injunction, however, staying the order pending appeal).

127. *See supra* notes 111–13 For a detailed history of the Snowden disclosures, see generally GREENWALD, *supra* note 107.

128. *Compare Klayman*, 957 F. Supp. 2d at 9–10 (granting, in part, a preliminary injunction on Fourth Amendment grounds, but staying the order pending appeal), *with Clapper*, 959 F. Supp. 2d at 742, 752, 757 (denying injunctive relief after holding the metadata collection was authorized by the statute and that the metadata collection did not constitute a search under the Fourth Amendment).

129. *See, e.g.*, *Klayman*, 957 F. Supp. 2d at 11 ("Specifically, plaintiffs allege that the Government has violated their individual rights under the First, Fourth, and Fifth Amendments of the Constitution and has violated the Administrative Procedure Act ('APA') by exceeding its statutory authority under FISA.").

130. *See id.* at 10 (quoting *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from Verizon Bus. Network Servs., Inc. on Behalf of MCI Commc'n Servs., Inc. d/b/a Verizon Bus. Servs., No. BR 13–80 at 2 (FISA Ct. Apr. 25, 2013)); *see also In re* Application No. BR 06-05, 2006 U.S. Dist. LEXIS 101368, at *1–2 (FISA Ct. May 24, 2006). The FISC would reauthorize this program every ninety days

On June 2, 2015, the U.S. Congress passed new legislation, the USA FREEDOM Act, intended to help resolve the legal dispute and to bring the NSA's bulk telephony metadata collection program under tighter regulation.[131] Proponents of the USA FREEDOM Act contend that the new law corrects the primary statutory and constitutional deficiencies of the bulk metadata collection program under Section 215 of the USA PATRIOT Act.[132] The law was passed two years after the Snowden disclosures and less than four weeks after the U.S. Court of Appeals for the Second Circuit determined in *Clapper* that the NSA had exceeded the scope of its statutory authority in impermissibly reading Section 215 to include bulk telephony metadata collection.[133]

Specifically, the USA FREEDOM Act requires the government to seek from the FISC orders for metadata records directly held by companies after identifying a specific person, account, address, or other specific identifier as a subject of a specific investigation.[134]

If the order is granted, the telecommunications provider or other corporate provider must produce the metadata records pursuant to a specific investigation.[135] In particular, the Act seeks to end the prior

following the original authorization which was granted in 2006. *See* Slobogin, *supra* note 23, at 1757.

131. *See supra* notes 11–12.

132. *See, e.g.*, Presidential Statement on Congressional Passage of the USA FREEDOM Act, 2015 DAILY COMP. PRES. DOC. 1 (June 2, 2015); Press Release, Representative Jim Sensenbrenner, Goodlatte, Conyers, Sensenbrenner, Nadler Applaud Clean Passage of the USA FREEDOM Act in the Senate (June 2, 2015), https://sensenbrenner.house.gov/2015/6/goodlatte-conyers-sensenbrenner-nadler-applaud-clean-passage-of-the-usa-freedom-act-in-the-senate [https://perma.cc/9RST-FEFL].

133. Edward Snowden's disclosures were first published on June 5, 2013, although some media reports date the disclosures as first published on June 6, 2013, with varying time zones. Greenwald, *supra* note 17; *see also* Mirren Gidda*, Edward Snowden and the NSA Files – Timeline*, GUARDIAN (Aug. 21, 2013, 5:54 PM), http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline [https://perma.cc/KWN8-PHYB]. The Second Circuit issued its decision on May 7, 2015. ACLU v. Clapper, 785 F.3d. 787, 792 (2d Cir. 2015).

134. USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 101(a)(3), 129 Stat. 268, 269–70 (codified at 50 U.S.C. § 1861(b)(2)(C) (2016)) ("[An] application for the production on a daily basis of call detail records . . . conducted to protect against international terrorism. "a statement of facts showing that . . . (1) there are reasonable grounds to believe that the call detail records sought to be produced based on the specific selection term required . . . are relevant to such investigation; and (ii) there are facts giving rise to a reasonable, articulable suspicion that such specific selection term is associated with a foreign power or an agent of a foreign power.").

135. *See, e.g.*, USA FREEDOM Act of 2015, § 101(b), 129 Stat. at 270; Steinhauer & Weisman, *supra* note 21 ("The storage of those records now shifts to the phone companies, and the government must petition a special federal court [FISC] for permission to search them."). Because the FISC orders may remain largely classified,

practice of allowing the NSA to collect bulk telephony metadata records and then store the records for future use.[136] In other words, under Section 215, bulk metadata collection came first and the querying of the database by the NSA came later on an as-needed basis, effectively allowing the NSA to control the maintenance and use of the bulk telephony metadata records.[137] Congress found this practice objectionable because it gave the NSA apparently unfettered access to the metadata.[138] Subsequently, Congress attempted to end it by placing a restraint on the government's ability to collect records by forcing the government to seek the production of the metadata records directly from the corporate entity (e.g., telecommunications company or Internet provider) in the USA FREEDOM Act.[139]

exactly how the USA Freedom Act will be implemented may remain unknown to the public. *See, e.g.*, § 602(a), 129 Stat. at 281 (allowing declassification for opinions that include "a significant construction or interpretation of any provision of law, including any novel or significant construction or interpretation of the term 'specific selection term', and, consistent with that review, make publicly available to the greatest extent practicable each such decision, order, or opinion").

136. *See* Cole, *supra* note 101 (explaining that under the USA FREEDOM Act, "the phone companies, not the NSA, would store the data"). Applications for orders to produce phone metadata records now must contain:

> (C) [A] statement of facts showing that—
>
> (i) there are reasonable grounds to believe that the call detail records sought to be produced based on the specific selection term required under subparagraph (A) are relevant to such investigation; and
>
> (ii) there is a reasonable, articulable suspicion that such specific selection term is associated with a foreign power engaged in international terrorism or activities in preparation therefor, or an agent of a foreign power engaged in international terrorism or activities in preparation therefor.

USA FREEDOM Act of 2015, § 101(a)(3)(C), 129 Stat. at 270.

137. *See* ACLU v. Clapper, 785 F.3d 787, 797 (2d Cir. 2015) ("The government explains that it uses the bulk metadata collected pursuant to these orders by making 'queries' using metadata 'identifiers' (also referred to as 'selectors'), or particular phone numbers that it believes, based on 'reasonable articulable suspicion,' to be associated with a foreign terrorist organization . . . . The identifier is used as a 'seed' to search across the government's database; the search results yield phone numbers, and the metadata associated with them that have been in contact with the seed.")

138. *See* Dan Froomkin, *For the First Time Since 9/11, Congress Checks the Security State*, INTERCEPT (June 1, 2015, 9:47 AM), https://theintercept.com/2015/06/01/first-time-since-911-congress-checks-security-state/ [https://perma.cc/P6Z6-FDJR] (quoting Sen. Ron Wyden, D-Ore., as saying that, "[t]onight the collection of phone records of millions of innocent Americans will end" and "[t]he demise of this dragnet surveillance is a victory for the principle that Americans do not need to sacrifice liberty to have security").

139. *See e.g.*, H.R. REP. NO. 114-109, pt. 1, at 8–10, 17–18 (2015); 160 CONG. REC. H4793 (daily ed. May 22, 2014) (statement of Rep. Bob Goodlatte) ("The USA FREEDOM Act makes clear that the government cannot indiscriminately acquire Americans' call detail records and creates a new, narrowly tailored process for the

Next, by requiring the NSA to articulate specific information for the person, account, address, or other precise identifier that is the subject of a particular investigation, the USA FREEDOM Act seeks to limit the scope of records sought by the government.[140] This contrasts with the prior practice, under Section 215 of the USA PATRIOT Act, where the metadata collection purportedly could proceed in an indiscriminate and suspicionless fashion.[141] The bulk collection justification under Section 215 by the government arguably allowed the NSA to collect all metadata on all calls, regardless of whether a specific person, account, or address was under investigation.[142] In enacting the USA FREEDOM Act, Congress appeared to agree with the Second Circuit in *Clapper* that Section 215 could not be reasonably read to allow all telephony metadata as "relevant" to an investigation.[143] Therefore, the USA FREEDOM

collection of these records."); 159 CONG. REC. S6052–54 (daily ed. July 30, 2013) (statement of Sen. Tom Udall) (calling for a targeted approach where the service providers maintain databases to meet national security needs while protecting Americans' privacy); Cole, *supra* note 101.

140. *See* USA FREEDOM Act of 2015, § 101(a)(3)(C), 129 Stat. at 270 (requiring the necessary statement of facts to relate to a "specific selection term").

141. *See, e.g.*, *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted], No. BR 06-05, 2006 U.S. Dist. LEXIS 101368, at *3 (FISA Ct. May 24, 2006) ("To the extent practicable, the Custodians of Records of [TEXT REDACTED] shall produce to NSA an electronic copy upon service of the appropriate secondary order, and continue production on an ongoing daily basis thereafter for the duration of this order, unless otherwise ordered by the Court, of the following tangible things: all call-detail records or 'telephony metadata' created by such companies as described above."); *see also* Klayman v. Obama, 957 F. Supp. 2d 1, 30 (D.D.C. 2013) (characterizing the bulk metadata collection program as allowing the Government to "indiscriminately collect[] [subscribers'] telephony metadata along with the metadata of hundreds of millions of other citizens without any particularized suspicion of wrongdoing"), *rev'd on other grounds*, 800 F.3d 559 (D.C. Cir. 2015).

142. *See, e.g.*, *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted], No. BR 13-80, 2013 U.S. Dist. LEXIS 147002, at *1–4 (FISA Ct. Apr. 25, 2013) (requiring the redacted party, which was soon revealed to be Verizon Business Network Services, Inc., to produce all daily telephony metadata to the FBI, except for communications "wholly originating and terminating in foreign countries"); Bart Forsyth, *Banning Bulk: Passage of the USA FREEDOM Act and Ending Bulk Collection*, 72 WASH. & LEE L. REV. 1307, 1312 (2015) ("With the bulk collection of telephony metadata, the government's statement of facts [showing relevancy] merely articulates a supposed value in collecting data on every call. There [is nothing] to differentiate calls that are more likely to relate to the government's investigation from every other call made by innocent Americans.").

143. *See* ACLU v. Clapper, 785 F.3d 787, 810–21 (2d Cir. 2015) (finding the government's argument that metadata is "'relevant' because they may allow the NSA, at some unknown time in the future . . . to identify information that *is* relevant" to be "unprecedented and unwarranted"); *see, e.g.*, Forsyth, *supra* note 142, at 1312 ("The government's interpretation of the section is so broad that it ultimately conflates relevance

Act, unlike Section 215 of the USA PATRIOT Act, appears to require a minimum demonstration that the metadata is related to a specific entity that is the subject of a specific investigation in order to establish that the metadata is "relevant" to that specific investigation.[144]

Prior to enactment of the Act, the NSA was allowed to seek records associated with up to three "hops" from the original "seed."[145] It is estimated that the "three-hop analysis" could result in the potential to query millions of phone records.[146] The USA FREEDOM Act further limited the scope of the records that could be requested by restricting the number of "hops" from an original "seed" to two

with utility—the records are relevant because the government believes it needs them. This is not a standard at all.").

144. *See* Klayman v. Obama, 142 F. Supp. 3d 172, 180 (D.D.C. 2015) ("[T]he USA FREEDOM Act expressly prohibits the Government from obtaining telephony metadata in bulk.").

145. President Obama implemented a revision from three "hops" to two "hops" prior to the enactment of the USA FREEDOM Act., Presidential Remarks on United States Signals Intelligence and Electronic Surveillance Programs, 2014 DAILY COMP. PRES. DOC. 7 (Jan. 17, 2014) ("Effective immediately, we will only pursue phone calls that are two steps removed from a number associated with a terrorist organization instead of the current three."). President Obama also took additional action to limit the querying of the database of telephony metadata prior to the USA FREEDOM Act. *Id*. ("And I have directed the Attorney General to work with the Foreign Intelligence Surveillance Court so that during this transition period, the database can be queried only after a judicial finding or in the case of a true emergency.").

146. The "three-hop" analysis was revealed during congressional testimony on July 17, 2013 in the aftermath of the Snowden disclosures. Pete Yost, *Congress Expresses Anger Over NSA Surveillance Program*, BOS. GLOBE (July 18, 2013), https://www.bostonglobe.com/news/nation/2013/07/17/nsa-spying-under-fire-you-got-problem/Ev73I1XwPYtvD2WFZ6idGK/story.html [https://perma.cc/BX5C-GQGZ (dark archive)] ("For the first time, NSA Deputy Director John C. Inglis disclosed that the agency sometimes conducts what is known as three-hop analysis. That means the government can look at the phone data of a suspected terrorist, plus the data of all of the contacts, then all of those people's contacts, and all of those people's contacts."). The NSA explained that: "[w]ith three-hop analysis, [i]f the average person calls 40 unique people, three-hop analysis could allow the government to mine the records of 2.5 million Americans when investigating one suspected terrorist." *Id*. The United States District Court for the District of Columbia explained further:

> In plain English, this means that if a search starts with telephone number (123) 456–7890 as the "seed," the first hop will include all the phone numbers that (123) 456–7890 has called or received calls from in the last five years (say, 100 numbers), the second hop will include all the phone numbers that each of *those* 100 numbers has called or received calls from in the last five years (say, 100 numbers for each one of the 100 "first hop" numbers, or 10,000 total), and the third hop will include all the phone numbers that each of *those* 10,000 numbers has called or received calls from in the last five years (say, 100 numbers for each one of the 10,000 "second hop" numbers, or 1,000,000 total).

Klayman v. Obama, 957 F. Supp. 2d 1, 16 (D.D.C. 2013) (citation omitted).

"hops," or in other words, the FISC may order the production of "the call detail records associated with the initial telephone number [the "seed"] and the records associated with the records returned in the initial hop."[147] The first "hop" is comprised of all of the records associated with the "seed"; the second "hop" is comprised of all of the records associated with the first "hop."[148] Bart Forsyth deconstructs this concept further:

> A second "hop" does not include an individual listed in a telephone contact list, or on a personal device that uses the same wireless router as the seed, or that has similar calling patterns as the seed. Nor does it exist merely because a personal device has been in the proximity of another personal device. These types of information are not maintained by telecommunications carriers in the normal course of business and, regardless, are prohibited under the definition of 'call detail records' [under the USA FREEDOM Act].[149]

Finally, the USA FREEDOM Act implemented changes to the FISC, including allowing for the appointment of "amicus curiae" in FISC matters involving novel and significant interpretations of the law,[150] and requiring more rigorous declassification reviews of FISC decisions.[151]

Importantly, however, the Act has been criticized as being inadequate to its purpose.[152] The criticism warrants careful attention

147. Forsyth, *supra* note 142, at 1339–40 (discussing Section 501 of the USA FREEDOM Act).

148. *Id.* at 1339 n.149.

149. *Id.*

150. Section 401 of the USA FREEDOM Act authorizes the presiding judge of the FISC to appoint at least five individuals to serve as "amicus curiae" to offer expertise in the application of the law to new technologies. Pub. L. No. 114-23, sec. 401, § 103, 129 Stat. 268, 279–81 (2015) (codified as amended at 50 U.S.C. § 1803 (2016)). The amici attorneys are eligible for security clearances and "will be tasked with making arguments addressing privacy and civil liberties, and will have access to relevant materials, including government applications, petitions, and motions [subject to being eligible for any necessary security clearances]." PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., RECOMMENDATIONS ASSESSMENT REPORT 5 (2016), https://www.pclob.gov/library/Recommendations_Assessment_Report_20160205.pdf [https://perma.cc/Q6ZV-PVT6].

151. *Id.* at 8 ("[T]he USA FREEDOM Act now requires that the government will conduct a declassification review of each new decision of the FISC and FISCR 'that includes a significant construction or interpretation of any provision of law,' . . . and that the government will make declassified versions of these opinions publicly available to the greatest extent practicable.").

152. *See, e.g.*, David Greene & Mark Jaycox, *Op-ed: Why the EFF is Pulling its Support for the USA FREEDOM Act*, ARS TECHNICA (May 12, 2015, 3:25 PM), http://arstechnica.com/tech-policy/2015/05/op-ed-why-the-eff-is-pulling-its-support-for-the-usa-freedom-act/ [https://perma.cc/Y82T-YUGU]; Neema Singh Guliani, *What's Next for*

in that the Act may not be sufficient to correct the statutory and constitutional deficiencies of Section 215 of the USA PATRIOT Act. Specifically, the Act may not curb bulk metadata collection for reasons that include, but are not limited to, the following three considerations. First, some argue that the Section 215 bulk telephony metadata program, as a "warrant"-based program (e.g., subject to FISC orders), was less problematic than warrantless bulk metadata collection programs.[153] Thus, the primary focus of statutory reform,

Surveillance Reform After the USA FREEDOM Act, ACLU (June 3, 2015, 6:15 PM), https://www.aclu.org/blog/washington-markup/whats-next-surveillance-reform-after-usa-freedom-act [https://perma.cc/M46T-NT85]. The USA Freedom Act, we hope, is only the beginning of this new era. The coalition that helped to advance the USA Freedom Act must now work to advance additional reforms. This includes:

> Urging both the president and Congress to rein in surveillance under Executive Order 12333, which has been used to collect information about millions of Americans absent any judicial process[;]
>
> Reforming Section 702 of the Foreign Intelligence Surveillance Act (set to expire in 2017), which allows the government to collect the content of Americans' communications with individuals abroad[;]
>
> Reforming other authorities, such as the administrative subpoena statutes, which have been used for bulk collection in the past[;]
>
> Further reforming the authorities addressed in the USA Freedom Act, including Section 215, FISA's pen-register and trap-and-trace provisions, and national security letters[;]
>
> Rejecting efforts to expand surveillance through cybersecurity information-sharing legislation.

Id; *see also* Kurt Opshal & Rainey Reitman, *A Floor, Not a Ceiling: Supporting the USA FREEDOM ACT as a Step Towards Less Surveillance*, ELECTRONIC FRONTIER FOUND. (Nov. 14, 2013), https://www.eff.org/deeplinks/2013/11/floor-not-ceiling-supporting-usa-freedom-act-step-towards-less-surveillance [https://perma.cc/LS9U-TLVR] ("It does not touch problems like NSA programs to sabotage encryption standards, it does not effectively tackle the issue of collecting information on people outside of the United States, and it doesn't address the authority that the government is supposedly using to tap the data links between service provider data centers, such as those owned by Google and Yahoo.").

153. *See, e.g.*, 161 CONG. REC. E883 (daily ed. June 11, 2015) (statement of Hon. Ted Poe) (claiming that the USA FREEDOM Act would not end bulk surveillance because it "does nothing to limit government spying under Section 702 of the FISA Amendments Act"); AMOS TOH, FAIZA PATEL & ELIZABETH GOITEIN, BRENNAN CTR. FOR JUSTICE, OVERSEAS SURVEILLANCE IN AN INTERCONNECTED WORLD 34 (2016), https://www.brennancenter.org/sites/default/files/publications/Overseas_Surveillance_in_an_Interconnected_World.pdf [https://perma.cc/B3UZ-TDHD] (discussing privacy impact of NSA's surveillance activities through Executive Order 12333 and lack of transparency of such activities); Ashley Gorski & Patrick C. Toomey, *Unprecedented and Unlawful: The NSA's "Upstream" Surveillance*, JUSTSECURITY (Sept. 19, 2016), https://www.justsecurity.org/33044/unprecedented-unlawful-nsas-upstream-surveillance/ [https://perma.cc/8Y4S-KY37] (challenging whether "Upstream" surveillance is authorized

according to some experts, should be on the warrantless collection of metadata and content data that was also revealed under the Snowden disclosures as justified under Section 702 of the Foreign Intelligence Surveillance Act Amendments Act ("FAA").[154] Second, some scholars note that statutory reform is a necessary but not a sufficient step toward the proper regulation of big data cyber surveillance methods.[155] They observe "that the Fourth Amendment must evolve along with" the statutory regime in order to properly restrain new and emerging surveillance methods, of which bulk metadata collection is

by the Foreign Intelligence Surveillance Act Amendments Act); Rainey Reitman, *The New USA FREEDOM Act: A Step in the Right Direction, but More Must Be Done*, ELECTRONIC FRONTIER FOUND. (Apr. 30, 2015), https://www.eff.org/deeplinks/2015/04/new-usa-freedom-act-step-right-direction-more-must-be-done [https://perma.cc/2H93-2ZCF] ("The new USA [FREEDOM] Act does not address Section 702 of the FISA Amendments Act, the problematic 2008 law that the government uses for PRISM and 'upstream' mass surveillance."); John Napier Tye, *Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans*, WASH. POST (July 18, 2014), https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html [https://perma.cc/TF9H-54NF] (explaining that although U.S. persons communications may not be targeted under Executive Order 12333, the executive order explicitly authorizes their retention if collected "incidentally" (with incidentally being "an NSA term of art") during a lawful overseas foreign intelligence investigation).

154. *See, e.g.*, Margulies, *supra* note 23, at 67–68. As a result of "sunset" clauses, Section 215 of the USA PATRIOT Act was set to expire on June 1, 2015, whereas Section 702 of the FISA Amendments Act was not set to expire until 2017. PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, § 2(a), 125 Stat. 216, 216 (codified in scattered sections of 50 U.S.C.); *see also* 50 U.S.C. § 1881a (2012). Because Section 215 preceded Section 702 in expiration, Section 215 appeared to take precedence as a matter of legislative reform. *See, e.g.,* Timothy Edgar, *Without USA Freedom Act, NSA Could Resume Bulk Collection Even if Patriot Act Provisions Expire*, LAWFARE (May 30, 2015, 5:20 PM), https://www.lawfareblog.com/without-usa-freedom-act-nsa-could-resume-bulk-collection-even-if-patriot-act-provisions-expire [https://perma.cc/62RH-HKEF]; Denise E. Zheng, *Electronic Surveillance After Section 215 of the USA Patriot Act*, CTR. FOR STRATEGIC & INT'L STUDIES (June 1, 2015), http://csis.org/publication/electronic-surveillance-after-section-215-usa-patriot-act [https://perma.cc/SQ8F-QURT]. Nevertheless, the FISA Amendments Reauthorization Act passed by floor vote on January 11, 2018. An Act to Amend the Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 115-118, 132 Stat. 3 (2018).

155. *See, e.g.*, Donohue, *Bulk Metadata Collection*, *supra* note 23, at 821; Donohue, *Section 702*, *supra* note 23, at 264–65. Professor Donohue recognized the need for a Fourth Amendment analysis, as well as the tension that exists when collecting programs are either seemingly performing the analysis themselves or are not fully understood such that human analysts can properly dispel Fourth Amendment concerns. *See* Donahue, *Bulk Metadata Collection*, *supra* note 23, at 821 ("[I]t appears that neither the NSA nor FISC had an adequate understanding of how the algorithms operate. Nor did they understand the type of information that had been incorporated into different databases, and whether they had been subjected to the appropriate legal analysis before data mining.").

but one.[156] Third, experts contend that strict compliance with the USA FREEDOM Act will not act as a constraint on metadata collection.[157] Each of these criticisms will be briefly summarized below.

First, beyond the Section 215 bulk telephony metadata program—which constituted bulk metadata collection pursuant to an order issued by the FISC—other authorities appear to have been interpreted by the intelligence community to allow for warrantless bulk metadata collection.[158] From the Snowden disclosures, it appears that in some instances the NSA saw neither the need to resort to the FISC to seek query-specific orders nor the express need to seek data from a third-party provider (e.g., a telecommunications corporation or Internet provider).[159] Under Section 702's "UPSTREAM"

156. *See, e.g.*, Jennifer Granick, *Prediction: Fourth Amendment Evolves in 2014*, JUST SECURITY (Dec. 31, 2013, 4:32 PM), https://www.justsecurity.org/5195/prediction-fourth-amendment-evolves-2014 [https://perma.cc/F2QM-5GNX] ("A consensus seems to be emerging that the Fourth Amendment must evolve along with technology and government surveillance capabilities.").

157. *See, e.g.*, Forsyth, *supra* note 142, at 1339; Ted Poe & Rand Paul, *Poe, Rand: NSA Bulk Collection of Data Tramples Our Rights*, HOUS. CHRON. (May 22, 2015, 9:20 PM), http://www.chron.com/opinion/outlook/article/Poe-Rand-NSA-bulk-collection-of-data-tramples-6282272.php [https://perma.cc/N8DW-6UW9] (claiming that the USA FREEDOM Act would not end bulk surveillance because it "does nothing to limit government spying under Section 702 of the FISA Amendments Act"). The USA FREEDOM Act allows FISC to order companies to produce up to two "hops." H.R. REP. NO. 114-109, pt. 1, at 17 (2015). The new authority in the in the USA FREEDOM Act was "designed to allow the government to search telephone metadata for possible connections to international terrorism—[however, it] does not preclude the government's use of standard business records orders under Section 501 to compel the production of business records, including call detail records." *Id*. at 18.

158. *See, e.g.*, Barton Gellman, Julie Tate & Ashkan Soltani, *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, WASH. POST. (July 5, 2014), https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html [https://perma.cc/BRQ8-4CAD]; Elizabeth Goitein, *Don't Lose Track: Here's What's Going on with the NSA*, BRENNAN CTR. FOR JUSTICE (July 8, 2014), https://www.brennancenter.org/analysis/dont-lose-track-heres-whats-going-nsa [https://perma.cc/4RDZ-SHHP].

159. From the Snowden disclosures, it appears that metadata surveillance is potentially justified under several legal authorities: Section 215 of the USA PATRIOT Act, Section 702 of FISA Amendments Act, and Executive Order 12333. Section 215 of the USA PATRIOT Act authorized the collection of "tangible things" that were relevant to an authorized investigation "to protect against international terrorism or clandestine intelligence activities." USA PATRIOT ACT of 2001, Pub. L. No. 107-56, sec. 215, § 501(a)(1), 115 Stat. 272, 287 (codified as amended at 50 U.S.C. § 1861 (2012)). Section 215 of the USA PATRIOT Act expired on June 1, 2015, and was replaced by the USA FREEDOM Act. Jeremy Diamond, *Patriot Act Provisions Have Expired: What Happens Now?*, CNN (June 1, 2015, 10:48 AM), https://www.cnn.com/2015/05/30/politics/what-happens-if-the-patriot-act-provisions-expire/index.html [https://perma.cc/BNP6-E49Q].

collection program, for instance, it was revealed that the NSA has the capacity to directly intercept bulk metadata and collection the content of communications traveling through fiber-optic cables that comprise the so-called "Internet backbone."[160] The NSA justified direct tapping of the fiber-optic cables to collect metadata—specifically "discrete wholly domestic communications" from U.S. citizens "that are neither to, from, [or regarding] a targeted selector"—by citing its authority to collect foreigners' data, and suggested that the data collected on U.S. persons through Section 702 was considered "incidental" and not purposeful and, thus, lawful.[161] The federal courts have not yet had an opportunity to determine whether this reading of Section 702 is permissible.[162]

Section 702 of FISA Amendments Act authorizes the Attorney General and the Director of National Intelligence to target non-U.S. persons "reasonably believed to be located outside the United States" for surveillance. FISA Amendments Act of 2008, Pub. L. No. 110-261, sec. 101, § 702, 122 Stat. 2436, 2437–48 (codified as amended at 50 U.S.C. § 1881a (2012)). Executive Order 12333 delegates to the Attorney General the power to authorize intelligence gathering pursuant to collection, dissemination and retention protocols set forth by the Order. Exec. Order No. 12333, § 2.5, 46 Fed. Reg. 59,941, 59,951 (Dec. 4, 1981), *as amended by* Exec. Order No. 13284 § 18, 68 Fed. Reg. 4075, 4077 (Jan. 23, 2003), Exec. Order No. 13355, 69 Fed. Reg. 53,593 (Aug. 27, 2004), *and* Exec. Order No. 13470, 73 Fed. Reg. 45,325 (July 30, 2008).

160. *See, e.g.*, James Ball, *Edward Snowden NSA Files: Secret Surveillance and Our Revelations So Far*, GUARDIAN (Aug. 21, 2013, 3:36 PM), http://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations [https://perma.cc/7SGK-NMR9]; Craig Timberg, *NSA Slide Shows Surveillance of Undersea Cables*, WASH. POST (July 10, 2013), https://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html [https://perma.cc/J6KY-76TK] (describing NSA slide that articulates UPSTREAM as accessing "communications on fiber cables and infrastructure as data flows past").

161. *See* [Redacted], 2011 U.S. Dist. LEXIS 157706, at *104 (FISA Ct. Oct. 3, 2011) ("The government stresses that the non-target communications of concern here (discrete wholly domestic communications and other discrete communications to or from a United States person or a person in the United States that are neither to, from, nor about a targeted selector) are acquired incidentally rather than purposefully."); *see also* James Ball & Spencer Ackerman, *NSA Loophole Allows Warrantless Search for US Citizens' Emails and Phone Calls*, GUARDIAN (Aug. 9, 2013, 12:08 PM), http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls [https://perma.cc/SA8E-8KXD].

162. *See, e.g.*, Donohue, *Section 702*, *supra* note 23, at 259–63 ("The petitioner's concern with incidental collections is overblown. It is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful. The government assures us that it does not maintain a database of incidentally collected information from non-targeted United States persons, and there is no evidence to the contrary. On these facts, incidentally collected communications of non-targeted United States persons do not violate the Fourth Amendment.") (quoting *In re* Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1015 (FISA Ct. Rev. 2008) (citations omitted))); *see also* Joshua A.T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981, 1025–26 (2014) (citing United States v. Mohamud, 941 F. Supp. 2d 1303 (D. Or.

Second, under the Fourth Amendment, it is unresolved under what circumstances the collection of metadata may constitute an unreasonable search or seizure.[163] The Fourth Amendment's third-party doctrine may be interpreted by the Supreme Court to allow for bulk metadata collection.[164] Further, the USA FREEDOM Act expressly limits bulk telephony metadata collection only—it does not appear to limit the type of metadata that can be generated by emails, Internet searches and web-browsing history, social media network activities, or information retained by smart technologies and other electronic devices.[165]

And, third, so long as the underlying presumption of efficacy persists, the intelligence community will likely collect the bulk metadata that it perceives it needs to serve purportedly mission-

2013)). In several cases, the defendant challenged the permissibility of the government withholding secret NSA surveillance evidence during discovery. Fairfield & Luna, *supra* at 1026 n.294.

163. *See, e.g.*, Klayman v. Obama, 142 F. Supp. 3d 172, 195–98 (D.D.C. 2015) (concluding plaintiff's claim that Section 215 program is unconstitutional under the Fourth Amendment has a likelihood of success on the merits and ordering injunction, blocking the final weeks of the Section 215 program prior to the implementation of the USA FREEDOM Act's reforms to metadata collection), *staying order*, 2015 WL 9010330 (D.C. Cir. 2015), *rehearing denied en banc*, 805 F.3d 1148 (D.C. Cir. 2015) (mem.); United States v. Moalin, No. 10cr4246 JM, 2013 U.S. Dist. LEXIS 164038, at *21 (S.D. Cal. Nov. 18, 2013) (holding that there is no reasonable expectation of privacy in telephony metadata under the Fourth Amendment).

164. *See, e.g.*, ACLU v. Clapper, 959 F. Supp. 2d 724, 751–52 (S.D.N.Y. 2013) ("[W]hen a person voluntarily conveys information to a third party, he forfeits his right to privacy in the information . . . . The collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep [of bulk telephony metadata collection] into a Fourth Amendment search."), *vacated*, 785 F.3d 787 (2d Cir. 2015); *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things, No. BR 15-75, 2015 WL 5637562, at *9 (FISA Ct. June 29, 2015) ("Prior FISC opinions have unanimously concluded that the production of call detail records to the government does not constitute a search under the Fourth Amendment, relying on [*Smith v. Maryland*]." (citing 442 U.S. 735 (1979)).

165. USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 101, 129 Stat. 268, 269–71 (2015) (codified at 50 U.S.C. § 1861(b)(2) (2016)). An argument could be made that the USA FREEDOM Act pertains to all metadata records and is not intended to regulate only telephony metadata collection in that Section 103 is titled, "Prohibition on the Bulk Collection of All Tangible Things." *See id.* However, the USA FREEDOM Act expressly refers to the regulation of "call detail records" in Section 101, thereby suggesting that the focus of the statute is on bulk telephony metadata collection. *Id*. Further, the USA FREEDOM ACT appears to limit its restrictions to bulk collection of domestic records and not bulk collection of foreign records, or records collected outside of the U.S. *See, e.g.*, Donohue, *Section 702*, *supra* note 23, at 139–53 (explaining that bulk collection methods can proceed under multiple legal authorities including Section 702 of FISA Amendments Act and Executive Order 12333); Margaret Hu, *Taxonomy of the Snowden Disclosures*, 72 WASH. & LEE L. REV. 1679, 1689–90 (2015).

critical counterterrorism objectives.[166] Procedurally, this can occur through technical compliance with the USA FREEDOM Act. The intelligence community, under the USA FREEDOM Act, may request orders from the FISC in a manner that may elicit a volume of metadata records on par with volumes achieved under Section 215's bulk telephony metadata collection program.[167] Despite Congress's attempts to statutorily curtail bulk metadata collection, intelligence agencies can still do so by working within and around the procedural parameters of the USA FREEDOM Act (e.g., the intelligence community may: delegate bulk metadata collection to other agencies, contractors, and entities, such as state and local law enforcement; purchase bulk metadata; negotiate direct access to metadata through

166. *See, e.g.*, Hu, *supra* note 102, at 773 (describing the expansion of "collect-it-all" data tools); Granick, *supra* note 156 (describing how without Fourth Amendment restrictions, the economics and technology of mass surveillance will encourage the government to continue".

167. *See* Schlanger, *supra* note 39, at 129 ("[T]he FISA Court now signs off on a massive program of targeted surveillance of foreigners—including when their communication is with an American."). The USA FREEDOM Act was criticized as potentially ineffective because the Act attempts to eliminate bulk collection through requiring the NSA to limit its request for data through a "specific selection term" restriction. *See, e.g.*, H.L. Pohlman, *The NSA FREEDOM Act?*, WASH. POST (May 27, 2014), https://www.washingtonpost.com/news/monkey-cage/wp/2014/05/27/the-nsa-freedom-act/ [https://perma.cc/3BHW-JYZJ] ("Their first concern, and the one most widely noted, is with the new definition of the kinds of 'specific selection terms' that the National Security Agency (NSA) could use when applying for court orders for the production of call detail records from private phone companies. What will NSA be searching for?"). Under the USA FREEDOM Act, particularly controversial was how to define "specific selection term" as a requirement for the basis of production of data and as a method to limit bulk collection of data. *See, e.g.*, Forsyth, *supra* note 142, at 1335–36. "[T]here was no aspect of the bill that garnered more intense focus than the definition of specific selection term. It was primarily this definition that led many technology companies and privacy groups to pull their support for the USA FREEDOM Act after it first passed the House in 2014." *Id.* at 1336. Bart Forsyth, chief of staff to Congressman F. James Sensenbrenner, explained the controversy this way: "By requiring a specific selection term, the USA FREEDOM Act therefore, by definition, ended bulk collection. But would this new limitation be sufficient in practice?" *Id.* at 1335 (footnote omitted). The USA FREEDOM Act limits the definition of a "specific selection term" so that it "cannot be used to identify an 'electronic service provider' or a 'broad geographic area.'" *Id.* at 1337 (citing USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 107(k)(4)(A)(i)–(ii), 129 Stat. at 273). "[T]he key to the new legal standard is that the specific selection term must be 'used to limit, to the greatest extent reasonably practicable, the volume of tangible things sought consistent with the purpose for seeking the tangible things.'" *Id.* (quoting USA FREEDOM Act, Pub. L. No. 114-23, § 107(k)(4)(A)(i)(II), 129 Stat. at 274.). "The [specific selection term] is, therefore, not intended to put a cap on the total amount of records, but instead, to limit the number of records to the greatest extent possible." *Id.* at 1337–38 (citing 161 CONG. REC. S2772 (daily ed. May 12, 2015)).

cooperative relationships with telecommunications and Internet providers; etc.).[168]

Consequently, under the USA FREEDOM Act, it is unclear whether bulk metadata collection will cease and, thus, whether mass suspicion-less tracking of metadata by the intelligence community will continue in an under-regulated manner.

III. POST-USA FREEDOM ACT

Absent any Supreme Court decision addressing the issue, the government has argued that the NSA's bulk telephony metadata program could continue temporarily.[169] Immediately after Congress passed the USA FREEDOM Act and President Barack Obama signed the Act into law on June 2, 2015, the DOJ filed a motion with the FISC seeking permission to extend the NSA's bulk telephony metadata collection program for an additional 180 days.[170] The motion cited a need to ensure an "orderly transition" from the prior bulk telephony metadata collection program under Section 215 of the

168. *See, e.g.*, Julia Angwin et al., *AT&T Helped U.S. Spy on Internet on a Vast Scale*, N.Y. TIMES (Aug. 15, 2015), http://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html?_r=0 [https://perma.cc/9QUZ-MM82 (dark archive)]; Ryan Deveraux, Glenn Greenwald & Laura Poitras, *Data Pirates of the Caribbean: The NSA is Recording Every Cell Phone Call in the Bahamas*, INTERCEPT (May 19, 2014, 12:37 PM), https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/ [https://perma.cc/G6MP-2BF8]; Glenn Greenwald et al., *Microsoft Handed the NSA Access to Encrypted Messages*, GUARDIAN (July 12, 2013, 3:04 AM), http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data [https://perma.cc/4Y4T-8A7K]; Brad Heath, *U.S. Secretly Tracked Billions of Calls for Decades*, USA TODAY (Apr. 8, 2015, 10:36 AM), http://www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-operation/70808616/ [https://perma.cc/JQ9R-MS2V] ("For more than two decades, the Justice Department and the Drug Enforcement Administration amassed logs of virtually all telephone calls from the USA to as many as 116 countries linked to drug trafficking, current and former officials involved with the operation said"); Jeremy Scahill & Josh Begley, *The Great SIM Heist: How Spies Stole the Keys to the Encryption Castle*, INTERCEPT (Feb. 19, 2015, 2:25 PM), https://theintercept.com/2015/02/19/great-sim-heist/ [https://perma.cc/ZPL7-5ZEN]; Craig Timberg & Ellen Nakashima, *Agreements with Private Companies Protect U.S. Access to Cables' Data for Surveillance*, WASH. POST (July 6, 2013), https://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html?tid=a_inl [https://perma.cc/3AQA-SWCZ].

169. *See* Memorandum of Law at 1, *In Re* Application of the FBI for an Order Requiring the Prod. of Tangible Things, No. BR 15-75, 2015 WL 5637562 (FISA Ct. June 29, 2015) (arguing that "Section 1861, as amended by the USA FREEDOM Act, authorizes the [FISA] Court to approve the Government's application for the bulk production of call detail records for a 180 day transition period," and that "such authorization is appropriate notwithstanding the Second Circuit's recent panel opinion in [*Clapper*]").

170. *Id.*

USA PATRIOT Act, and the Justice Department argued that the USA FREEDOM Act expressly allows for an extension of bulk telephony metadata collection for an additional 180 days.[171]

The key question centers upon what the program now resembles, given that the USA FREEDOM Act went into effect as of December 1, 2015. Put another way, the question remains whether the NSA has facilitated an "orderly transition" from the Section 215 bulk telephony metadata collection program to another similar bulk telephony metadata collection program that is technically within compliance with the USA FREEDOM Act.[172] As mentioned above, the Act does not prohibit the delegation of bulk telephony metadata collection to other agencies and entities; requesting orders from the FISC in a manner that achieves a similar volume to the prior bulk metadata collection program; and intensifying metadata collection under Section 702 of the FAA and Executive Order 12333.[173] Shifting the justification for bulk metadata collection to other legal authorities allows the NSA and other intelligence organizations to collect in the absence of order requirements now specified under the USA FREEDOM Act.

Moreover, the USA FREEDOM Act only speaks to bulk telephony metadata collection that had previously been justified under Section 215 of the USA PATRIOT Act.[174] The Act does not regulate mass metadata collection generated by emails, Internet searches and web-browsing history, social media network activities, and information retained by smart technologies and other electronic devices, as mentioned above.[175] So long as the intelligence community perceives bulk metadata is needed to support a big data

171. *Id.* at 5–6 ("Congress recognized the need for an orderly transition period that preserves an important foreign intelligence collection capability until the Government may effectively avail itself of the new provisions for a targeted production.").

172. *See supra* notes 155–56 and accompanying text.

173. *See supra* notes 165–68 and accompanying text.

174. *See* Cole, *supra* note 101 ("The bill is addressed almost entirely to the NSA's domestic surveillance, but the vast majority of the agency's spying is conducted overseas and directed at foreigners. Under those programs, which are not touched by the USA [FREEDOM] Act, the agency has, for example, recorded the contents of every phone call for a year in some countries; vacuumed up massive amounts of Internet data on wholly innocent persons; and collected the contents of phone calls, e-mails, and Internet activity of millions of innocent people. Because these measures are targeted at foreigners, they don't generate the same level of concern here as at home. But these programs implicate our rights, too, as they routinely intercept communications between US citizens and foreign persons. Even an e-mail from Poughkeepsie to Peoria may be routed through France or England without our knowing it, and thus be subject to NSA interception.").

175. *See* MacAskill, *supra* note 36.

cybersurveillance architecture[176] that has been built for over a decade—an architecture that, based upon modest estimates, reflects an investment of billions of dollars[177]—the task of bringing bulk metadata collection under closer oversight is an extraordinarily difficult one.

It is particularly instructive to point out that in *ACLU v. Clapper*,[178] the U.S. Court of Appeals for the Second Circuit concluded with a discussion of the constitutional issues raised by the bulk telephony metadata program, noting that, on this issue, "the Supreme Court's jurisprudence is in some turmoil."[179] But instead of trying to resolve that turmoil, the Second Circuit rested its decision on its statutory findings and noted that the legislative branch is "better positioned than the courts . . . to pass judgment on the value of the telephone metadata program as a counterterrorism tool."[180] Yet, importantly, in its motion filed with the FISC days after the passage of the USA FREEDOM Act, the DOJ argued that the U.S. Court of Appeals for the Second Circuit opinion in *Clapper* is not binding on the FISC.[181] The government argued that "[the FISA] Court's analysis of Section 215 reflects the better interpretation of the statute" and called on the court to continue to apply it.[182] Only one judge in one federal court, Judge Leon in the District Court of Washington, D.C., held that bulk metadata collection posed a violation of the Fourth Amendment.[183]

The circuit split stems from diametrically opposing views of whether bulk metadata collection is protected by the Fourth

176. Experts increasingly describe big data surveillance in architectural terms. *See, e.g.*, BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 48 (2015) ("This has evolved into a shockingly extensive, robust, and profitable surveillance architecture.").

177. "[The National Archives, Information Security Oversight Office] has studied how much the federal government spends just to keep secrets secret. The price tag: $10 billion a year." DANA PRIEST & WILLIAM M. ARKIN, TOP SECRET AMERICA: THE RISE OF THE NEW AMERICAN SECURITY STATE 24 (2011). "The budget [for intelligence] had been estimated to be $75 billion a year, which did not include all the military's spending on counterterrorism and intelligence." *Id.* at 103.

178. 785 F.3d 787 (2d Cir. 2015).

179. *Id.* at 821–23 (referring to Fourth Amendment jurisprudence leading up to, and including, *United States v. Jones*, 565 U.S. 400 (2012)).

180. *Id.* at 824.

181. Memorandum of Law, *supra* note 169, at 7; *see also* Spencer Ackerman, *Obama Lawyers Asked Secret Court to Ignore Public Court's Decision on Spying*, GUARDIAN (June 9, 2015, 7:00 AM), http://www.theguardian.com/world/2015/jun/09/obama-fisa-court-surveillance-phone-records [https://perma.cc/7ST9-J7HE].

182. Memorandum of Law, *supra* note 169, at 7.

183. Klayman v. Obama, 957 F. Supp. 2d 1, 32 (D.D.C. 2013), *rev'd on other grounds*, 800 F.3d 599 (D.C. Cir. 2015).

Amendment and whether the third-party doctrine controls such collection. The core of the third-party doctrine, established in *Smith v. Maryland*,[184] is that an individual lacks a subjective expectation of privacy in data shared with a third party—which in this case is the telephone provider.[185] In the Southern District of New York, Judge Pauley determined that the third-party doctrine eliminated the possibility of a Fourth Amendment violation because customers shared their telephony metadata with a third party[186]—Verizon—thus, there was no reasonable expectation of privacy in the metadata.[187] As noted above, the Second Circuit reversed Judge Pauley's decision on appeal, but only by avoiding the constitutional issue and deciding the case on statutory grounds.[188]

Judge Leon chose to confront the constitutional issue, finding that the third-party doctrine from *Smith v. Maryland* was not controlling. *Katz v. United States*[189] requires a two-step analysis: beginning with the question of whether the individual had a reasonable expectation of privacy, one then moves to the question of whether society would ratify that expectation as reasonable.[190] Under this test, an individual seemingly could not have a reasonable expectation of privacy in the metadata from her telephone because the data had been shared with a third party, the telephone company; therefore, the bulk telephony metadata program would not be unconstitutional. But Judge Leon contended that such a result would be unreasonable and contrary to the spirit of *Katz*, arguing that the technological changes "have resulted in a *greater* expectation of privacy and a recognition that society views that expectation as reasonable."[191] His decision, while bold, ultimately was overturned by the D.C. Circuit: based on standing concerns, that court vacated the preliminary injunction that the district court had granted.[192]

184. 442 U.S. 735 (1979).

185. *Id*. at 743–44.

186. *Id.*

187. ACLU v. Clapper, 959 F. Supp. 2d 724, 751 (S.D.N.Y. 2013), *vacated*, 785 F.3d 787, 792 (2d Cir. 2015).

188. *See supra* notes 178–80 and accompanying text (discussing the Second Circuit's opinion).

189. 389 U.S. 347 (1967).

190. *Id.* at 361 (Harlan, J., concurring) (clearly outlining the twofold test).

191. *Id.*

192. Obama v. Klayman, 800 F.3d 559, 563 (D.C. Cir. 2015) (explaining that "the facts marshaled by plaintiffs do not fully establish that their own metadata was ever collected").

CONCLUSION

The USA FREEDOM Act is a significant legislative accomplishment, reflecting an impressive bipartisan effort. The clear intent of the USA FREEDOM Act is to impose meaningful limits on bulk metadata collection. The extent to which it will succeed is an open question, but the law has included important oversight protections. Because the FISC operates in a shroud of secrecy, the USA FREEDOM Act is an accomplishment in that it both increases transparency measures and implements additional accountability measures. By allowing for the declassification of certain FISC opinions, the USA FREEDOM Act may increase the chance that the public can understand how the FISC is interpreting the USA FREEDOM Act. The USA FREEDOM Act allows for public reporting by service provider companies, therefore, theoretically, significant increases in collection may be reported by the private sector. The USA FREEDOM Act also reflects structural changes to how the FISC operates. It allows for the appointment of amicus curiae to represent alternative perspectives to the court. Further, under the Section 215 program, bulk metadata collection was authorized by the FISC as a wholesale program, however, queries of the data were not court-approved. Under the USA FREEDOM Act, queries now are subject to FISC approval.

The reforms to Section 215 of the USA PATRIOT Act, which was used to justify the bulk telephony metadata collection program revealed by the Snowden disclosures, appear to apply to the government as a whole, not just the NSA; and arguably, the text of the law on its face could be read to apply to the collection of all records—not just metadata or even telephony metadata. The law also attempts to limit potential bulk collection under the Pen Register, or Trap and Trace, authority and national security letters.[193]

Yet, bulk metadata collection is largely under-regulated by the current federal legislative scheme governing U.S. surveillance activities. The USA FREEDOM Act's "specific selection term"

193. *See ODNI Announces Transition to New Telephone Metadata Program*, OFFICE DIR. NAT'L INTELLIGENCE (Nov. 27, 2015), https://icontherecord.tumblr.com/post/134069716908/odni-announces-transition-to-new-telephone [https://perma.cc/KWL3-L2LC] (explaining how "[t]he Act . . . banned bulk collection under Section 215 of the USA PATRIOT Act, under the pen register and trap and trace provisions found in Title IV of Foreign Intelligence Surveillance Act (FISA), or pursuant to National Security Letters").

requirement could be interpreted broadly;[194] the definition of a query could be expanded;[195] "incidental" collection could still sweep in metadata collection in bulk;[196] and limiting the collection to two "hops" means potentially millions of "call detail records" can still be collected under the Act.[197] U.S. federal courts appear to be conflicted about how to treat metadata collection under the federal scheme that is intended to subject it to proper oversight. Moreover, it is unclear how metadata surveillance falls within the preexisting Fourth Amendment jurisprudence of the U.S. Constitution. In implementing the USA FREEDOM Act, the FISC has declined to follow, for example, the U.S. Court of Appeals for the Second Circuit's opinion in *Clapper*, and suggested that it is awaiting resolution of the issue of the constitutionality of metadata surveillance by the Supreme Court.[198]

194. *See, e.g.,* Reitman, *supra* note 153 ("[T]he specific selection term is the basis for the query that the government uses when it collects records. A broad selection term ('People in California' or 'People with Verizon phones') would mean massive record collection, but carefully constructed and defined specific selection terms would strictly limit the collection.").

195. *See, e.g.*, Elizabeth Goitein, *The FBI's Warrantless Surveillance Back Door Just Opened a Little Wider*, JUST SECURITY (Apr. 21, 2016), https://www.justsecurity.org/30699/fbis-warrantless-surveillance-door-opened-wider/ [https://perma.cc/2A4V-M74R].

196. *See, e.g.*, Faiza Patel, *Bulk Collection Under Section 215 Has Ended . . . What's Next?*, JUST SECURITY (Nov. 30, 2015), https://www.justsecurity.org/27996/bulk-collection-ended-whats-next/ [https://perma.cc/ABQ5-LKF9]; Patrick Toomey, *Obama Administration Embraced Legal Theories Broader Than John Yoo's,* JUST SECURITY (Apr. 7, 2016), https://www.justsecurity.org/30460/obama-administration-embraced-legal-theories-broader-john-yoos/ [https://perma.cc/VG7F-76Z6].

197. *See, e.g.*, *supra* notes 146–50 and accompanying text.

198. *See In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things, No. BR 15-75, 2015 WL 5637562, at *7 (FISA Ct. June 29, 2015) (stating that the Second Circuit's ruling is not binding on the FISC; Order declining to follow Second Circuit approach).

> The Court is aware that, prior to enactment of the USA FREEDOM Act, the Second Circuit in *Clapper* rejected the government's arguments that the call detail records acquired under the NSA program were relevant to an authorized investigation other than a threat assessment as required by section 501(b)(2)(A) and (c)(1) of FISA. However, Second Circuit rulings are not binding on the FISC, and this Court respectfully disagrees with that Court's analysis, especially in view of the intervening enactment of the USA FREEDOM Act. As Judge Eagan stated: "Taken together, the [section 501] provisions are designed to permit the government wide latitude to seek the information it needs to meet its national security responsibilities, but only in combination with specific procedures for the protection of U.S. person information that are tailored to the production and with an opportunity for the authorization to be challenged.

Id. at *15 (alteration in original). On June 5, 2017, the Court granted certiorari in Carpenter v. United States, 819 F.3d 880 (6th Cir. 2016). *See* Carpenter v. United States, No. 16-402, 2017 WL 2407484 (U.S. June 5, 2017). In *Carpenter*, the Court will decide

Finally, there is no conclusive evidence thus far that bulk metadata collection—bulk telephony or non-telephony metadata such as bulk biometric data collection or bulk biometric metadata collection—is efficacious.[199] Consequently, an assessment of the efficacy of these rapidly emerging metadata collection methods should become integral to any future statutory reform, and future oversight and compliance reform efforts.[200] Efficacy determinations can also serve an important role in an evolution of the constitutional inquiry under the Fourth Amendment.[201] Even with passage of the USA FREEDOM Act, metadata surveillance is likely to continue to proceed under-regulated until the courts resolve the constitutionality of newly emerging methods of metadata surveillance and bulk metadata collection. Consequently, the cybersurveillance potential of smart body cameras or smart glasses worn by law enforcement offers and important case study for understanding how the USA FREEDOM Act is unable to regulate bulk biometric data collection of bulk biometric metadata collection.

"[w]hether the warrantless seizure and search of historical cell phone records revealing the location and movements of a cell phone user over the course of 127 days is permitted by the Fourth Amendment." Petition for a Writ of Certiorari at 10–11, *Carpenter*, 819 F.3d 880 (No. 16-402).

199. *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., *supra* note 39, at 11 ("Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation.").

200. *See generally* Hu, *supra* note 102, at 786 (explaining why a scientific critique "may aid in assessing the efficacy of big data-driven national security policymaking").

201. *See id.* at 808–16 (analyzing relevant case law and explaining how better understanding the efficacy of these programs may affect Fourth Amendment concerns in this area).