William & Mary Bill of Rights Journal

Volume *26 (2017-2018)*
Issue 2 *Symposium: Big Data, National Security, and the Fourth Amendment*

Article 6

December 2017

Horizontal Cybersurveillance Through Sentiment Analysis

Margaret Hu

HORIZONTAL CYBERSURVEILLANCE THROUGH SENTIMENT ANALYSIS

Margaret Hu*

ABSTRACT

This Essay describes emerging big data technologies that facilitate horizontal cybersurveillance. Horizontal cybersurveillance makes possible what has been termed as "sentiment analysis." Sentiment analysis can be described as opinion mining and social movement forecasting. Through sentiment analysis, mass cybersurveillance technologies can be deployed to detect potential terrorism and state conflict, predict protest and civil unrest, and gauge the mood of populations and subpopulations. Horizontal cybersurveillance through sentiment analysis has the likely result of chilling expressive and associational freedoms, while at the same time risking mass data seizures and searches. These programs, therefore, must be assessed as adversely impacting a combination of constitutional rights, such as simultaneously affecting both First and Fourth Amendment freedoms.

INTRODUCTION 362
I. RELATIONSHIP BETWEEN BIG DATA NATIONAL SECURITY POLICY AND BIG DATA CYBERSURVEILLANCE 366
A. Overview of Big Data National Security Policy 366
B. Overview of Horizontal Cybersurveillance 369
C. Horizontal Cybersurveillance Through Sentiment Analysis: Future Trajectory of Big Data National Security Policy 372
II. SOCIAL RADAR CASE STUDY: THE FUTURE OF BIG DATA NATIONAL SECURITY POLICY 374
A. Brief History of Horizontal Cybersurveillance Programs 375
B. Basic Mechanics of Social Radar 378
C. Current Status of Social Radar and Social Radar-Type Programs . . . 379
CONCLUSION 381

* Associate Professor of Law, Washington and Lee University School of Law. I would like to extend my deep gratitude to those who graciously offered comments on the research, including Andrew Christensen, David Gray, Stephen Henderson, and Steve Miskinis. In addition, this research benefitted greatly from the discussions generated from the *William & Mary Bill of Rights Journal* 2017 Symposium: *Big Data, National Security, and the Fourth Amendment*. Many thanks to the research assistance of Alexandra Klein, Kirby Kreider, and Carroll Neale. All errors and omissions are my own.

INTRODUCTION

Big data[1] facilitates frictionless surveillance[2] for the sake of cybersurveillance.[3] In big data cybersurveillance regimes, anyone engaging in digital communications can be either a source of data to fuel the cybersurveillance machine or a legitimate target of investigation.[4] Because of the scope of developing technologies, even public presentation of one's face or body can be subjected to data storage, collection, and analysis.[5] Thus, theoretically, any activity or non-activity can be captured by cybersurveillance technologies that in turn subject the individual to a much larger cybersurveillance apparatus. Other technologies seek to capture and analyze content for community sentiment, potential crimes, or threats of terrorism.[6] Such technologies include "social radar" technologies, which can "rapidly achieve situational awareness of the human environment, identify alternative courses of action—whether through words or deeds—and better understand the potential outcomes of those actions."[7]

---

[1] The phenomenon of what has been termed the "big data revolution" has been the focus of extensive and important research. *See, e.g.*, BIG DATA CHALLENGES: SOCIETY, SECURITY, INNOVATION AND ETHICS (Anno Bunnik et al. eds., 2016) [hereinafter BIG DATA CHALLENGES]; BIG DATA: AN EXPLORATION OF OPPORTUNITIES, VALUES, AND PRIVACY ISSUES (Cody Agnellutti ed., 2014); JAMES R. KALYVAS & MICHAEL R. OVERLY, BIG DATA: A BUSINESS AND LEGAL GUIDE (2015); PRIVACY IN THE MODERN AGE: THE SEARCH FOR SOLUTIONS (Marc Rotenberg et al. eds., 2015) [hereinafter PRIVACY SOLUTIONS]; danah boyd & Kate Crawford, *Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon*, 15 INFO., COMM. & SOC'Y 662 (2012).

[2] *See, e.g.*, ZYGMUNT BAUMAN & DAVID LYON, LIQUID SURVEILLANCE: A CONVERSATION (2013); Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721 (2014).

[3] *See* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 3 (2008) ("Government's increasing use of surveillance and data mining is a predictable result of accelerating developments in information technology. As technologies that let us discover and analyze what is happening in the world become ever more powerful, both governments and private parties will seek to use them." (citations omitted)).

[4] *See, e.g.*, AnnaMaria Andriotis & Emily Glazer, *Banks Weigh Shift from Equifax: TransUnion, Experian Are Poised to Pick Up Business in the Wake of Big Data Breach*, WALL ST. J., Sept. 13, 2017, at B14.

[5] *See, e.g.*, James Risen & Laura Poitras, *N.S.A. Collecting Millions of Faces from Web Images*, N.Y. TIMES, June 1, 2014, at A1 (discussing how the Snowden disclosures showed the NSA used facial recognition technology on images taken from the Internet); Nate Berg, *What Happens When You Ask to See CCTV Footage?*, GUARDIAN (Sept. 22, 2015, 2:30 EDT), https://www.theguardian.com/cities/2015/sep/22/cctv-cameras-capture-almost-every-move-on-city-streets-what-happens-when-you-ask-to-see-the-footage [https://perma.cc/2YJZ-8D3C] ("In the United States, where citywide surveillance systems, police car-mounted automated license plate readers and body-worn cameras are being adopted across the country, many are concerned about the lack of regulations controlling how this data is being collected, stored and made available, especially when the collection is happening in public spaces.").

[6] *See infra* Part I.

[7] *Social Radar Technologies*, MITRE CORP., https://www.mitre.org/research/technology-transfer/technology-licensing/social-radar-technologies [https://perma.cc/ESX4-7B69] (last visited Dec. 4, 2017).

Constitutional law scholars Jack Balkin and Sanford Levinson warn that the "National Surveillance State" is upon us.[8] In the National Surveillance State, a ubiquitous surveillance governance system "will be developed by Congress and particularly by military and civilian bureaucracies within the executive branch."[9] Such a state would rely on "surveillance, data collection, collation, and analysis to identify problems, to head off potential threats, to govern populations, and to deliver valuable social services."[10] Balkin explains that the National Surveillance State will use surveillance and analysis conducted by private parties as a feature of governance.[11] Surveillance technologies developed by corporations, as well as by defense contractors, have been provided to public law enforcement agencies.[12]

In the United States, the law has yet to match the speed with which cybersurveillance technologies have developed, and many scholars have theorized how the law can—or should—change to keep pace with technology and to preserve constitutional protections.[13] The Constitution reflects metaphysical ambitions[14] and a natural

---

[8] *See generally* Jack M. Balkin & Sanford Levinson, *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 FORDHAM L. REV. 489 (2006).

[9] *Id.* at 490.

[10] Balkin, *supra* note 3, at 3.

[11] *Id.* at 4.

[12] *See generally* Heidi Boghosian, *The Business of Surveillance*, 39 A.B.A. HUM. RTS. 2, 2–5, 23 (2013).

[13] *See, e.g.*, Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326 (2015); Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547 (2017); Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805 (2016); Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681 (2011); 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 (2013); David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013); Stephen E. Henderson, *Real-Time and Historic Location Surveillance After* United States v. Jones*: An Administrable, Mildly Mosaic Approach*, 103 J. CRIM. L. & CRIMINOLOGY 803 (2013); Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011); Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005 (2010); Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285 (2015); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich L. Rev. 311 (2012); Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205; Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527 (2017); Stephanie K. Pell & Christopher Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J.L. & TECH. 134 (2013); 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 (SPECIAL ISSUE) 1 (2012); Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614 (2011).

[14] *See* ARCHIBALD COX, THE COURT AND THE CONSTITUTION 26–27, 39 (1987) (describing the open-ended nature of the language of the Amendments to the Constitution).

rights philosophy.[15] As individuals' lives have become increasingly intertwined with technology,[16] constitutional harms have become increasingly hard to define. Thus, individual rights, as articulated by the Bill of Rights, must be interpreted as interrelated in the National Surveillance State.[17] The interrelationship of constitutional amendments is critical as constitutional harms become entangled by mass surveillance, including horizontal cybersurveillance.

The relationship between the First and Fourth Amendments, for example, is necessary to recognize in such a system of governance.[18] The First Amendment protects expressive and associational rights.[19] The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[20] The Fourth Amendment has been recognized as affording "a constitutionally protected reasonable expectation of privacy."[21] Courts have recognized that the two protections are linked—survival of First Amendment rights is

---

[15] *See* Chester James Antieau, *Natural Rights and the Founding Fathers—The Virginians*, 17 WASH. & LEE L. REV. 43, 43, 46–49 (1960) (discussing how the Founding Fathers were aware of natural rights, as evidenced through their writings); *see also* COX, *supra* note 14, at 36, 38 (noting the influences on the Constitutional Convention).

[16] *See, e.g.*, VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 11 (2013) (describing the ways individuals use technology in their everyday lives).

[17] Multiple scholars have started to look at the specific implications of the emerging policing technologies that are the hallmarks of the National Surveillance State, such as the chilling of expression, loss of agency and autonomy, and the mass conformity risks. *See, e.g.*, NEIL RICHARDS, INTELLECTUAL PRIVACY: RETHINKING CIVIL LIBERTIES IN THE DIGITAL AGE (2015); Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014); Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904 (2013); Deven R. Desai, *Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding*, 90 NOTRE DAME L. REV. 579 (2014); Nita A. Farahany, *Searching Secrets*, 160 U. PA. L. REV. 1239 (2012); Margot E. Kaminski & Shane Whitnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465 (2015); Craig Konnoth, *An Expressive Theory of Privacy Intrusions*, 102 IOWA L. REV. 1533 (2017); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013); Scott Skinner-Thompson, *Performative Privacy*, 50 U.C. DAVIS L. REV. 1673 (2017); Kathleen M. Sullivan, *Under a Watchful Eye: Incursions on Personal Privacy*, *in* THE WAR ON OUR FREEDOMS: CIVIL LIBERTIES IN AN AGE OF TERRORISM 128, 131 (Richard C. Leone & Greg Anrig, Jr. eds., 2003).

[18] *See* Alex Abdo, *Why Rely on the Fourth Amendment to Do the Work of the First?*, 127 YALE L.J. F. 444 (2017); Nicole B. Cásarez, *The Synergy of Privacy and Speech*, 18 U. PA. J. CONST. L. 813 (2016).

[19] U.S. CONST. amend. I ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."); *see* Tinker v. Des Moines Indep. Cmty. Sch. Dist., 393 U.S. 503, 513 (1969); NAACP v. Alabama, 357 U.S. 449, 462 (1958).

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

[21] Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

dependent upon the protections of the Fourth Amendment.[22] The Fourth Amendment "provide[s] citizens with the privacy protection necessary for secure enjoyment of First Amendment liberties."[23]

Thus, as technologies are developed to track and analyze sentiment and expression,[24] it is essential to consider the potential effect of big data cybersurveillance on the Constitution and the impact of near-constant, real-time surveillance on a democracy.[25] As part of the Symposium *Big Data, National Security, and the Fourth Amendment*, this Essay preliminarily explores some constitutional challenges to the Fourth Amendment that may result in light of emerging big data technologies that facilitate horizontal cybersurveillance capacities. This Essay is descriptive in nature and, thus, it does not aim to offer a legal analysis of the impact of horizontal cybersurveillance. Rather, it offers a very brief overview of how national security policy is currently embracing the phenomena of sentiment analysis as a technological outgrowth of horizontal cybersurveillance.

This Essay proceeds in two parts. In Part I, this Essay describes how, increasingly, the military and the intelligence communities rely upon "collect-it-all" programs to enhance national security decision-making and counterterrorism policy. Part I focuses on how big data facilitates a synergistic and dependent relationship between national security decision-making and developments in cybersurveillance. Part II

---

[22] *See* Zurcher v. Stanford Daily, 436 U.S. 547, 565 (1978); Roaden v. Kentucky, 413 U.S. 496, 504 (1973); United States v. U.S. Dist. Court, 407 U.S. 297, 313–14 (1972); Stanford v. Texas, 379 U.S. 476, 485 (1965); *NAACP*, 357 U.S. at 462 ("[There is a] vital relationship between freedom to associate and privacy in one's associations."); Reporters Comm. for Freedom of Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1054 (D.C. Cir. 1978); *see also* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1587 (2004).

[23] *Reporters Comm.*, 593 F.2d at 1054.

[24] *See infra* Section I.C.

[25] Development of these new technologies could lead to increasingly complex constitutional issues in various areas, including algorithms, censorship, cyber hate, and the right to be forgotten. *See, e.g.*, DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (2014); ABRAHAM H. FOXMAN & CHRISTOPHER WOLF, VIRAL HATE: CONTAINING ITS SPREAD ON THE INTERNET (2013); Stuart Minor Benjamin, *Algorithms and Speech*, 161 U. PA. L. REV. 1445 (2013); Dawn Carla Nunziato, *Forget About It? Harmonizing European and American Protections for Privacy, Free Speech, and Due Process*, *in* PRIVACY AND POWER: A TRANSATLANTIC DIALOGUE IN THE SHADOW OF THE NSA-AFFAIR (Russell A. Miller ed., 2017); Jeffrey Rosen, *The Deciders: Facebook, Google, and the Future of Privacy and Free Speech*, *in* CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE 69 (Jeffrey Rosen & Benjamin Wittes eds., 2011); Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88 (2012); Eric Posner, *We All Have the Right to Be Forgotten*, SLATE (May 14, 2014, 4:37 PM), http://www.slate.com/articles/news_and_politics/view_from_chicago/2014/05/the_european_right_to_be_forgotten_is_just_what_the_internet_needs.html [https://perma.cc/9H38-SLVB]; Jeffrey Rosen, *The Delete Squad*, NEW REPUBLIC (Apr. 29, 2013), https://newrepublic.com/article/113045/free-speech-internet-silicon-valley-making-rules [https://perma.cc/HT5X-3PQ4].

explores how horizontal cybersurveillance makes possible what has been termed as "sentiment analysis." Sentiment analysis can be described as opinion mining and social movement forecasting. Through sentiment analysis, mass cybersurveillance technologies can be deployed to detect potential terrorism and state conflict, predict protest and civil unrest, and gauge the mood of populations and subpopulations.

The Essay concludes that horizontal cybersurveillance through sentiment analysis has the likely result of chilling expressive and associational freedoms, while at the same time risking mass data seizures and searches. These programs, therefore, must be assessed as adversely impacting a combination of constitutional rights, such as simultaneously affecting both First and Fourth Amendment freedoms. The blending of constitutional harms that results from new big data national security technologies must be protected through an interpretive blending of multiple Bill of Rights protections.

I. RELATIONSHIP BETWEEN BIG DATA NATIONAL SECURITY POLICY AND BIG DATA CYBERSURVEILLANCE

A. Overview of Big Data National Security Policy

Understanding big data cybersurveillance and big data governance[26] requires understanding big data. Although scholars have discussed its characteristics and complexities, big data does not have a specific definition.[27] Big data is often explained in terms of "three Vs"—volume, velocity, and variety—although other experts add other "Vs": vision, verification, and valuation.[28] Volume and variety refer to the capabilities of big data analysis to absorb vast amounts of data from a multitude of sources.[29] For big data tools to work effectively, they require enormous amounts of

---

[26] *See, e.g.*, Margaret Hu, *Biometric Surveillance and Big Data Governance*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 121 (David Gray & Stephen E. Henderson eds., 2017).

[27] *See, e.g.*, JULES J. BERMAN, PRINCIPLES OF BIG DATA: PREPARING, SHARING, AND ANALYZING COMPLEX INFORMATION xv–xvi (2013) (categorizing big data into the "three Vs"—volume, velocity, and variety); MAYER-SCHÖNBERGER & CUKIER, *supra* note 16, at 13 (describing big data as "messy, varie[d] in quality, and . . . distributed among countless servers around the world"); *see also The Big Data Conundrum: How to Define It?*, MIT TECH. REV. (Oct. 3, 2013), https://www.technologyreview.com/s/519851/the-big-data-conundrum-how-to-define-it/ [https://perma.cc/JDR9-882J] [hereinafter *Big Data Conundrum*] (listing the various definitions for "big data").

[28] *See* BERMAN, *supra* note 27, at xv. Regarding the veracity of the underlying data, it is important to remember, as then-Judge Gorsuch explained it: "Garbage in, garbage out." United States v. Esquivel-Rios, 725 F.3d 1231, 1234 (10th Cir. 2013).

[29] *See* Harry E. Pence, *What Is Big Data and Why Is It Important?*, 43 J. EDUC. TECH. SYS. 159, 161–62 (2014) (categorizing big data into the three Vs); *Volume, Velocity, Variety: What You Need to Know About Big Data*, FORBES (Jan. 19, 2012, 9:46 AM), https://www.forbes.com/sites/oreillymedia/2012/01/19/volume-velocity-variety-what-you-need-to-know-about-big-data/2/#219a250470a1 [https://perma.cc/JD55-Q5U5] (categorizing big data into the three Vs).

data.[30] Big data is not defined solely by the amount of data—it is also about the complexity of the data sets, and thus some argue that "the high degree of permutations and interactions within a data set . . . defines big data."[31] The three Vs require "cost-effective, innovative forms of information processing" with the goal of achieving "enhanced insight and decision making."[32] As defined by the National Science Foundation, "Big Data Science & Engineering" is about using information analysis and supervision to obtain information from "large, diverse, distributed and heterogeneous data sets."[33] Big data science permits the creation of data infrastructure as well as new algorithmic and analytic data tools.[34] Big data technologies are necessarily outside human capacity because big data requires supercomputing and machine learning—accordingly, humans require computer assistance, such as algorithms, to process the data.[35] To understand the shift in governance from a small data[36] surveillance[37] world to a big data[38] cybersurveillance[39] world, it is helpful to understand the distinctions between small data surveillance (vertical surveillance) and big data

---

[30] *See* Uthayasankar Sivarajah et al., *Critical Analysis of Big Data Challenges and Analytical Methods*, 70 J. BUS. RES. 263, 265 (2017).

[31] *See Big Data Conundrum*, *supra* note 27.

[32] John Pavolotsky, *Privacy in the Age of Big Data*, 69 BUS. LAW. 217, 217 (2013) (quoting Svetlana Sicular, *Gartner's Big Data Definition Consists of Three Parts, Not to Be Confused with Three "V"s*, FORBES (Mar. 27, 2013, 8:00 AM), https://www.forbes.com/sites/gartnergroup/2013/03/27/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs/#7bcebc4b42f6 [https://perma.cc/2E4C-T4DW]).

[33] NAT'L SCI. FOUND., NSF 12-499, CORE TECHNIQUES AND TECHNOLOGIES FOR ADVANCING BIG DATA SCIENCE & ENGINEERING (BIGDATA) 2 (2012), https://www.nsf.gov/pubs/2012/nsf12499/nsf12499.pdf [http://perma.cc/LU47-K366].

[34] *See id.*

[35] *See* MAYER-SCHÖNBERGER & CUKIER, *supra* note 16, at 11–12.

[36] "Small data" has been described, generally, "as solving discrete questions with limited and structured data, and the data are generally controlled by one institution." Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 329 n.6 (2015) (citing BERMAN, *supra* note 27, at 1–2). For a list of important recent works detailing the legal and privacy implications of transformative technological developments like the Internet and technological innovations in surveillance capacities, see Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV. 773, 776 n.2 (2015).

[37] In an earlier article, I used "the term ['small data surveillance'] . . . as a way to mark a contrast between traditional intelligence gathering methods (i.e., 'small data surveillance') and newly emerging intelligence methods that are digital data-driven, dependent upon supercomputing capacities, and capitalize on big data phenomena and tolls (i.e., 'big data surveillance')." Hu, *supra* note 36, at 776 n.3. I adopt the same definition here.

[38] Multiple authors have addressed the characteristics of "big data" and the challenges posed by big data technologies. *See generally, e.g.*, BIG DATA CHALLENGES, *supra* note 1; KALYVAS & OVERLY, *supra* note 1; PRIVACY SOLUTIONS, *supra* note 1.

[39] For a list of scholarship that "use[s] the term 'big data surveillance' to describe how surveillance methods are evolving in light of the emerging pervasiveness of big data technologies," see Hu, *supra* note 36, at 778 n.8.

surveillance (horizontal cybersurveillance and indiscriminate bulk collection of data).[40] Vertical surveillance begins with suspicion, often of a specific target, which leads to monitoring, surveillance, and search warrants.[41] Vertical collection is purpose-driven: it is about building an investigatory case to confirm or eliminate the suspicion that triggered the monitoring.[42] Horizontal data collection is radically different in scope and kind from vertical data collection. Horizontal data collection is often initiated without a specific target.[43] It is suspicionless cybersurveillance, which collects and digitally stores data for real-time or future analysis.[44] "Bulk" data collection, such as bulk "telephone metadata" collection, is one illustrative method of horizontal data collection.[45] Some analysts and scholars describe horizontal mass collection as a "'haystack-before-the-needle' approach."[46] Horizontal data collection methods emphasize collecting as much data as possible to connect the dots for meaningful connections or associations.[47]

In horizontal cybersurveillance, the goal is to collect as much data as possible for subsequent analysis.[48] Rob Kitchin explains that data-driven science is "more open to using a hybrid combination of abductive, inductive and deductive approaches to advance the understanding of a phenomenon."[49] Big data seeks correlation that can potentially provide predictive results.[50] In a national security context, big data may be utilized to predict crimes or terrorist attacks before they occur.[51] The ability to collect nearly unlimited amounts of data enables algorithms that may identify patterns

---

[40] *See* Hu, *supra* note 36, at 776 nn.2–3, 777 n.4 (discussing the importance of realizing the small and big data surveillance distinctions).

[41] *Id.* at 804, 832.

[42] *Id.*

[43] *Id.* at 832–33.

[44] *Id.*

[45] *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 5, 2013, 6:05 EDT), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [https://perma.cc/3RSS-D6SK].

[46] Stephen I. Vladeck, *Big Data Before and After Snowden*, 7 J. NAT'L SEC. L. & POL'Y 333, 334 (2014) (citing Rachel Levinson-Waldman, Opinion, *The Double Danger of the NSA's 'Collect It All' Policy on Surveillance*, GUARDIAN (Oct. 10, 2013, 10:19 EDT), http://www.theguardian.com/commentisfree/2013/oct/10/double-danger-nsa-surveillance [https://perma.cc/5DFN-FDTM]).

[47] *See* Hu, *supra* note 36, at 834–35.

[48] *See id.* at 802–05.

[49] Rob Kitchin, *Big Data, New Epistemologies and Paradigm Shifts*, 1 BIG DATA & SOC'Y 1, 5 (2014).

[50] *See generally* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION (2015); Danielle Keats Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1 (2014).

[51] *See* William C. Banks, *Next Generation Foreign Intelligence Surveillance Law: Renewing 702*, 51 U. RICH. L. REV. 671 (2017).

and, potentially, crime or terrorism.[52] The differences between vertical and horizontal collection methods, as well as the predictive potential of big data, provide insight into why intelligence communities have implemented and focused on "collect-it-all" programs,[53] as was revealed by the disclosures provided by former National Security Agency (NSA) contractor Edward Snowden.[54] The Snowden revelation demonstrated mass, indiscriminate bulk data collection from individuals without suspicion.[55] One of Snowden's disclosures contained an NSA slide that described the "collection posture" of the NSA: "'Collect it All,' 'Process it All,' 'Exploit it All,' 'Partner it All,' 'Sniff it All,' and, ultimately, 'Know it All.'"[56] Because big data analysis is capable of making broad connections, it motivates increasing data collection—the value of one piece of information is often unknown until it is connected to information that has already been obtained, or that might be obtained in the future.[57]

B. Overview of Horizontal Cybersurveillance

Because of the change in technological capacity with the rise of the Information Society, the vocabulary surrounding surveillance itself has changed. Data surveillance, described as "dataveillance,"[58] refers to monitoring or investigation of individual

---

[52] *See, e.g.*, Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 42–46 (2014) (describing how police departments in the United States can use data to predict criminal activity).

[53] *See* Mathew Ingram, *Even the CIA Is Struggling to Deal with the Volume of Real-Time Social Data*, GIGAOM (Mar. 20, 2013, 10:27 AM), https://gigaom.com/2013/03/20/even-the-cia-is-struggling-to-deal-with-the-volume-of-real-time-social-data [https://perma.cc/DG54-DLXY] [hereinafter CIA Presentation] (providing video from and a transcript of the CIA's Chief Technology Officer's speech at Gigaom's March 2013 conference).

[54] *See* Margaret Hu, *Taxonomy of the Snowden Disclosures*, 72 WASH & LEE L. REV. 1679, 1689–94 (2015). *See generally* GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE (2014); THE SNOWDEN READER (David. P. Fidler ed., 2015).

[55] *See generally* AFTER SNOWDEN: PRIVACY, SECRECY, AND SECURITY IN THE INFORMATION AGE (Ronald Goldfarb ed., 2015); DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE (2017).

[56] David Cole, Opinion, *'No Place to Hide' by Glenn Greenwald, on the NSA's Sweeping Efforts to 'Know It All,'* WASH. POST (May 12, 2014), https://www.washingtonpost.com/opinions/no-place-to-hide-by-glenn-greenwald-on-the-nsas-sweeping-efforts-to-know-it-all/2014/05/12/dfa45dee-d628-11e3-8a78-8fe50322a72c_story.html?=utm_term=.3bbb86d72687 [https://perma.cc/P59V-E297].

[57] RACHEL LEVINSON-WALDMAN, BRENNAN CTR. FOR JUSTICE, WHAT THE GOVERNMENT DOES WITH AMERICANS' DATA 17 (2013).

[58] Roger Clarke is generally credited with introducing the term "dataveillance" into academic discourse. *See* Roger A. Clarke, *Information Technology and Dataveillance*, 31 COMM. ACM 498, 498–99 (1988); *see also* MARTIN KUHN, FEDERAL DATAVEILLANCE: IMPLICATIONS

actions, activities, or communications through the use of information technology.[59] The complete capacities and potential consequences of this "new surveillance" are as yet not fully known.[60] What is understood is that mass dataveillance and cybersurveillance is possible because technology now exists that "datafie[s]"[61] virtually all information. Thus, social life, human activity, and knowledge can be quantified, digitized, retained indefinitely, and analyzed for connections and information.[62] The Snowden disclosures demonstrate why, in constitutional analysis, it is important to understand the differences between small data surveillance and big data cybersurveillance.[63] The Snowden disclosures and other revelations provided evidence of the extent to which the NSA and other agencies are increasingly using mass dataveillance and cybersurveillance tools,[64] in addition to traditional surveillance methods developed in a small data world.

FOR CONSTITUTIONAL PRIVACY PROTECTIONS 1–3 (2007) (examining constitutional implications of "knowledge discovery in databases" (KDD applications) through dataveillance); DAVID LYON, SURVEILLANCE STUDIES: AN OVERVIEW 16 (2007) ("Being much cheaper than direct physical or electronic surveillance [dataveillance] enables the watching of more people or populations, because economic constraints to surveillance are reduced. Dataveillance also automates surveillance. Classically, government bureaucracies have been most interested in gathering such data . . . .").

[59] *See* Clarke, *supra* note 58, at 499 (describing dataveillance as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons").

[60] *See* LYON, *supra* note 58, at 87–89.

[61] MAYER-SCHÖNBERGER & CUKIER, *supra* note 16, at 91–97.

[62] CIA Presentation, *supra* note 53. *See generally* JAMES GLEICK, THE INFORMATION: A HISTORY, A THEORY, A FLOOD (2011); DOUGLAS RUSHKOFF, PRESENT SHOCK: WHEN EVERYTHING HAPPENS NOW (2013).

[63] *See generally* Hu, *supra* note 36.

[64] The Snowden disclosures have included multiple high-profile revelations on newly emerging dataveillance tools, cybersurveillance methods, and information specific to their implementation. *See* Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html [https://perma.cc/6FZ3-XR6T]; Greenwald, *supra* note 45; Ellen Nakashima & Barton Gellman, *Court Gave NSA Broad Leeway in Surveillance, Documents Show*, WASH. POST (June 30, 2014), http://www.washingtonpost.com/world/national-security/court-gave-nsa-broad-leeway-in-surveillance-documents-show/2014/06/30/32b872ec-fae4-11e3-8176-f2c941cf35f1_story.html [https://perma.cc/475T-LQDD]; Scott Shane, *No Morsel Too Minuscule for All-Consuming N.S.A.*, N.Y. TIMES (Nov. 2, 2013), http://www.nytimes.com/2013/11/03/world/no-morsel-too-minuscule-for-all-consuming-nsa.html; T.C. Sottek & Janus Kopfstein, *Everything You Need to Know About PRISM: A Cheat Sheet for the NSA's Unprecedented Surveillance Programs*, VERGE (July 17, 2013), http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet [https://perma.cc/SXR6-VP5D].

In intelligence settings, cybersurveillance "collect-it-all"[65] tools can potentially create "digital avatars"[66]—virtual representations[67] of digital selves.[68] "Data self"[69] and "cyber self"[70] are used to describe an individual's online reputation. "Digital personhood,"[71] as described by scholars, means something entirely different. It describes the process by which "digital dossiers"[72] may be created to construct what has been variously described by scholars as a "data-double,"[73] "data image,"[74] "digital persona,"[75] or "electronic personality and digital self."[76] These terms are used to explain that in the Information Society, cybersurveillance is not aimed at "complete bodies," but rather in "fragments of data"[77] that can create a bigger and more complete picture of many individuals and their connections. Another related concept, the "proliferation of networked identities and selves," refers to preservation of the autonomous individual within the Information Society's vast infrastructure.[78]

---

[65] *See* Cole, *supra* note 56 ("In one remarkable [NSA] slide presented at a 2011 meeting of five nations' intelligence agencies and revealed here for the first time, the NSA described its 'collection posture' as 'Collect it All,' 'Process it All,' 'Exploit it All,' 'Partner it All,' 'Sniff it All' and, ultimately, 'Know it All.'").

[66] "The term 'digital avatar' is used often in the video gaming context, and most commonly refers to a digitally constructed representation of the computing user or, in some instance, the representation of the user's alter ego or character." Hu, *supra* note 36, at 779 n.11 (citing Hart v. Elec. Arts, Inc., 717 F.3d 141 (3d Cir. 2012)). "In *Hart v. Electronic Arts, Inc*., for example, a class action suit of college athletes alleged that their digital avatars and likeness had been unlawfully appropriated for profit by the video game developer, Electronic Arts, Inc." *Id.* (citing *Hart*, 717 F.3d 141).

[67] Virtual reality and augmented reality give rise to legal questions that span multiple legal disciplines. *See* David E. Fink & Jamie N. Zagoria, *VR/AR in a Real World*, 33 ENT. & SPORTS LAW. 1, 75–79 (2016); Mark A. Lemley & Eugene Volokh, *Law, Virtual Reality, and Augmented Reality*, 166 U. PA. L. REV. (forthcoming 2018).

[68] *See* DIGITAL TECHNOLOGIES OF THE SELF (Yasmine Abbas & Fred Dervin eds., 2009).

[69] *See* Robert Gordon, *The Electronic Personality and Digital Self*, 56 DISP. RESOL. J. 8, 14 (2001) (stating how the "digital self" allows one to "become whomever [one] want[s] to be in cyberspace" (emphasis removed)).

[70] *See* Chassitty N. Whitman & William H. Gottdiener, *The Cyber Self: Facebook as a Predictor of Well-Being*, 13 INT'L J. APPLIED PSYCHOANALYTIC STUD. 142 (2016).

[71] *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004).

[72] *See id.* at 1–2; Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1084 (2002).

[73] Kevin D. Haggerty & Richard V. Ericson, *The Surveillant Assemblage*, 51 BRIT. J. SOC. 605, 606, 611, 613, 616 (2000).

[74] LYON, *supra* note 58, at 87 (citing DAVID LYON, THE ELECTRONIC EYE: THE RISE OF SURVEILLANCE SOCIETY 19 (1994)).

[75] *See id.* at 87–88 (citing Roger Clarke, *The Digital Persona and Its Application to Data Surveillance*, 10 INFO. SOC'Y 77 (1994)).

[76] *See* Gordon, *supra* note 69, at 14.

[77] *See* LYON, *supra* note 58, at 88 (citing Haggerty & Ericson, *supra* note 73, at 612).

[78] For scholarship on this concept, see Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735, 1754 & n.71 (2015).

One alleged 2010 NSA document from the Snowden materials explained the possible function of digital selves: "'It's not just the traditional communications we're after: It's taking a full-arsenal approach that digitally exploits the clues a target leaves behind in their regular activities on the net to compile biographic and biometric information' that can help 'implement precision targeting.'"[79] Other information in the Snowden disclosures included discussions of biometric data collection[80]—fingerprints, irises, DNA, and facial recognition technology applied to digital photographs.[81] The "full-arsenal approach" of mass surveillance relies on data science[82] to pinpoint suspicious data and evidence of guilt in digital avatars.[83] These tools are heighted by the use of other cybersurveillance techniques, including sentiment analysis.[84]

C. Horizontal Cybersurveillance Through Sentiment Analysis: Future Trajectory of Big Data National Security Policy

The development of social media, as well as the proliferation of online media and big data tools, has led to technologies that are capable of tracking and identifying sentiment in societies and communities.[85] These tools are valuable in precrime ambitions.[86] After the terrorist attacks of September 11, 2001, policy began focusing on "precrime" decision-making, rather than prevention.[87] The capacities of big data

---

[79] Risen & Poitras, *supra* note 5, at A1.

[80] *Id.* "While once focused on written and oral communications, the N.S.A. now considers facial images, fingerprints and other identifiers just as important to its mission of tracking suspected terrorists and other intelligence targets, the documents show." *Id.*

[81] Biometrics is "[t]he science of automatic identification or identity verification of individuals using physiological or behavioral characteristics." JOHN R. VACCA, BIOMETRIC TECHNOLOGIES AND VERIFICATION SYSTEMS 589 (2007). For a list of sources exploring the emerging technology of biometrics and discussing its application and potential consequences, see Hu, *supra* note 36, at 781 n.18.

[82] "At its core, data science involves using automated methods to analyze massive amounts of data and to extract knowledge from them." *What Is Data Science?*, N.Y.U., https://datascience.nyu.edu/what-is-data-science/ [https://perma.cc/M7ET-NF8L] (last visited Dec. 4, 2017).

[83] For a careful examination of the legal implications of utilizing targeted killing policies and drone strikes as a crucial element of the United States' counterterrorism policy, see Hu, *supra* note 36, at 784 n.27 (citing multiple scholars, including Martin S. Flaherty, Oren Gross, Gregory S. McNeal, Matthew Craig, and Jennifer Daskal, who have thoroughly studied this subject area).

[84] *See* Walaa Medhat et al., *Sentiment Analysis Algorithms and Applications: A Survey*, 5 AIN SHAMS ENGINEERING J. 1093 (2014) (Egypt) (providing a detailed overview of sentiment analysis techniques).

[85] *See id.* at 1093; Ronen Feldman, *Techniques and Applications for Sentiment Analysis*, 56 COMM. ACM 82, 83–84 (2013) (describing how sentiment analysis works).

[86] *See* Hu, *supra* note 26, at 122 (stating that "*Minority Report*–type biometric surveillance systems and precrime rationales are now embedded in big data governance ambitions").

[87] *Id.* at 123.

make predictive analysis possible, thus incentivizing precrime governance programs and increasing the use of mass cybersurveillance technologies.[88]

Sentiment analysis purports to be a valuable tool in a precrime policing model. Sentiment analysis, also described as "opinion mining," is described as "the computational study of people's opinions, attitudes, and emotions toward an entity."[89] It can "analyze what a percentage of the population 'feels' about something, often by measuring the sentiments embedded in social media posts or by asking a community directly to share its feelings, thoughts, or opinions in a machine-readable way."[90] Other tools related to sentiment analysis include geofencing programs that collect public social media postings or track users' locations for commercial or ideological purposes.[91] Geofencing creates a "virtual fence" around an identified physical location.[92] This technology, when paired with social media, could permit sentiment analysis of a given location, as well as tracking and cybersurveillance of activities in the area based on social media activity.[93] Such tools raise understandable concerns about the problems of individual tracking and the potential for privacy violations, as well as interference with constitutionally protected activities.[94]

Programs intended to track and analyze population sentiment were in existence long before big data and were utilized in national security and military contexts. During World War II, social scientists tried "to predict national [behavior] as part of wartime operations."[95] These studies were intended to "enable American political

---

[88] *See generally id.*

[89] Medhat et al., *supra* note 84, at 1093.

[90] Sam Petulla, *Feelings, Nothing More than Feelings: The Measured Rise of Sentiment Analysis in Journalism*, NIEMAN LAB (Jan. 23, 2013, 10:00 AM), http://www.niemanlab.org/2013/01/feelings-nothing-more-than-feelings-the-measured-rise-of-sentiment-analysis-in-journalism/ [https://perma.cc/EAU4-TQJN].

[91] *See generally* Jonah Engel Bromwich et al., *Police Use Surveillance Tool to Scan Social Media, A.C.L.U. Says*, N.Y. TIMES (Oct. 11, 2016), https://www.nytimes.com/2016/10/12/technology/aclu-facebook-twitter-instagram-geofeedia.html; Matthew Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, ACLU (Oct. 11, 2016, 11:15 AM), https://www.aclu.org/blog/privacy-technology/internet-privacy/facebook-instagram-and-twitter-provided-data-access [https://perma.cc/B8H7-Z8LV]; Nicole Ozer, *Police Use of Social Media Surveillance Software Is Escalating, and Activists Are in the Digital Crosshairs*, ACLU (Sept. 22, 2016, 2:45 PM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/police-use-social-media-surveillance-software [https://perma.cc/T6KM-ZBWM].

[92] Jamie Wong et al., *An Android Geofencing App for Autonomous Remote Switch Control*, 11 INT'L J. COMPUTER & INFO. ENGINEERING 325, 325 (2017).

[93] *See* Bromwich et al., *supra* note 91; Cagle, *supra* note 91; Ally Marotti, *Chicago Police Used Geofeedia, the TweetDeck for Cops Under Fire from ACLU*, CHI. TRIB. (Oct. 13, 2016, 2:30 PM), http://www.chicagotribune.com/bluesky/originals/ct-geofeedia-police-surveillance-reports-bsi-20161013-story.html; Ozer, *supra* note 91.

[94] *See* Ozer, *supra* note 91.

[95] Mark Solovey, *Project Camelot and the 1960s Epistemological Revolution: Rethinking*

leaders to control beliefs and attitudes within target populations, both domestic and foreign."[96] Much of this research appeared to be targeted towards controlling communist influences in particular regions of the world.[97] Such military research demonstrated "a marked preference for quantitative analysis."[98]

In the 1960s, the U.S. military sponsored a study of revolutionary processes called "Project Camelot."[99] Camelot was a project of the Department of Defense, the Defense Science Board, and the U.S. Army; it was planned by the Special Operations Research Office (SORO).[100] Project Camelot's objectives were to (1) "devise procedures for assessing the potential for internal war within societies," (2) "identify with increased degrees of confidence those actions which a government might take to relieve conditions which are assessed as giving rise to a potential for internal war," and (3) "assess the feasibility of prescribing the characteristics of a system for obtaining and using the essential information needed for doing the above two things."[101] Essentially, Project Camelot attempted to engage in sentiment analysis regarding internal wars, determine how to reduce the tensions in a population, and discern how to make a system that would provide the information needed. Project Camelot was disbanded after rising international and political tensions,[102] but the notion of being able to predict possible crises has never disappeared; it has only increased following September 11.[103]

II. SOCIAL RADAR CASE STUDY: THE FUTURE OF BIG DATA NATIONAL SECURITY POLICY

In 2010, the Air Force published a paper[104] that it described as a "vision document" for a tool it referred to as "Social Radar."[105] It was inspired by the use of traditional military radar and other detection tools as a means to expand "situational awareness" by

---

the Politics-Patronage-Social Science Nexus, 31 SOC. STUD. SCI. 171, 177 (2001), http://journals.sagepub.com/doi/pdf/10.1177/0306312701031002003 [https://perma.cc/9F55-LWXL].

[96] *Id.*

[97] *Id.*

[98] *Id.*

[99] *Id.* at 180.

[100] *Id.*

[101] *Id.* at 180–81 (internal quotations omitted).

[102] *Id.* at 186 ("Within the United States, international outcry from abroad triggered a series of communications involving the US ambassador to Chile, the State Department, the military, and the White House, leading in July of 1965 to Camelot's cancellation.").

[103] *See* Steve Ressler, *Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research*, 2 HOMELAND SECURITY AFF. 1, 3 (2006), https://www.hsaj.org/articles/171 [https://www.perma.cc/QQG8-YJ9U].

[104] The document was authored by Dr. Mark Maybury, then chief scientist of the U.S. Air Force. *Dr. Mark T. Maybury: Vice President, Intelligence Portfolios, MITRE National Security Sector*, MITRE CORP., https://www.mitre.org/about/leadership/executive/dr-mark-t-maybury [https://perma.cc/PF8E-VRNV] (last visited Dec. 4, 2017).

[105] MARK MAYBURY, MITRE CORP., SOCIAL RADAR FOR SMART POWER 1 (2010), https://www.mitre.org/sites/default/files/pdf/10_0745.pdf [https://perma.cc/KYP4-2LL6].

enhancing ordinary human capabilities, such as sight.[106] The document explained that these tools, however, "are blind to human adversary attitudes and intentions and often even behaviors toward our messages and activities."[107] It further explained that while military technology is important, "soft power"—the ability "to encourage or motivate behavior"—is highly significant in an increasingly globally connected world.[108]

A. Brief History of Horizontal Cybersurveillance Programs

The development of big-data horizontal scanning programs facilitated mass cybersurveillance and big data governance, particularly in the wake of the September 11 attacks.[109] For example, a post-9/11 program, Total Information Awareness (TIA), later renamed Terrorism Information Awareness,[110] was a "collect it all" surveillance program.[111] TIA was a project of the Information Awareness Office, within the Department of Defense's Defense Advanced Research Projects Agency (DARPA).[112] TIA had preventive policing ambitions and endorsed mass data collection to assess and prevent future threats.[113] TIA was intended to "integrate advanced collaborative and decision support tools; language translation; and data search, pattern recognition, and privacy protection technologies into an experimental prototype network focused on the problems of countering terrorism through better analysis"[114] and decision-making. This program acknowledged human limitations—given the sheer amount of information available for analysis—and instead sought "a much more systematic methodological approach that automates many of the lower level functions that can

---

[106] *Id.* at 2.

[107] *Id.*

[108] *Id.* at 3.

[109] *See generally* Hu, *supra* note 78.

[110] NAT'L RESEARCH COUNCIL, PROTECTING INDIVIDUAL PRIVACY IN THE STRUGGLE AGAINST TERRORISM: A FRAMEWORK FOR PROGRAM ASSESSMENT 239 (2008).

[111] TIA was not referred to as a "Collect It All" program at the time of its conception. *See id.* at 239–49. Rather, this phrase is taken from the Snowden disclosures. *See* GREENWALD, *supra* note 54, at 97 (citing NSA slide from Snowden disclosures titled, "New Collection Posture" and quoting NSA data collection procedure as "Collect it All").

[112] *See* Nancy Murray, *Profiling in the Age of Total Information Awareness*, 52 RACE & CLASS 3, 6 (2010).

[113] DEF. ADVANCED RESEARCH PROJECTS AGENCY, REPORT TO CONGRESS REGARDING THE TERRORISM INFORMATION AWARENESS PROGRAM: IN RESPONSE TO CONSOLIDATED APPROPRIATIONS RESOLUTION, 2003, PUB. L. NO. 108-7, DIVISION M, § 111(B), at A-1 (2003), https://epic.org/privacy/profiling/tia/may03_report.pdf [https://perma.cc/X52X-3D4B] [hereinafter DARPA REPORT] ("[T]his program . . . would provide decision- and policy-makers with information and knowledge about terrorist planning and preparation activities that would aid in preventing future international terrorist attacks against the United States at home and abroad."); *see also* Matt Kessler, *The Logo that Took Down a DARPA Surveillance Project*, ATLANTIC (Dec. 22, 2015), https://www.theatlantic.com/technology/archive/2015/12/darpa-logos-information-awareness-office/421635/ [https://perma.cc/T6CX-Y4NM].

[114] *See* DARPA REPORT, *supra* note 113, at A-1.

be done by machines guided by the human users."[115] TIA, in short, intended to harness the power of big data and algorithms to provide greater efficiency in intelligence and analysis.[116] TIA was officially defunded in late 2003,[117] but experts theorized that the remnants of TIA survived in the NSA, ultimately leading to the types of programs that Edward Snowden revealed in 2013.[118]

Following the Snowden disclosures, bulk data collection became a matter of increasing public concern.[119] The existence of the Foreign Intelligence Surveillance Act (FISA)[120] and the PATRIOT Act[121] were not secrets—they operated pursuant to existing law. Even prior to the Snowden disclosures, people were already expressing concerns about the way in which surveillance had been conducted.[122]

In 2008, the U.S. Department of Defense (DoD) created the "Minerva Research Initiative,"[123] with the intent, in partnership with universities, "to improve DoD's basic understanding of the social, cultural, behavioral, and political forces that shape regions of the world of strategic importance to the [U.S.]"[124] Minerva engages in broad avenues of "research aimed at improving our basic understanding of security, broadly defined."[125] One Minerva project is a study managed by the U.S. Air Force Office of Scientific Research that "aims to develop an empirical model 'of the dynamics of social movement mobilization and contagions.'"[126] Aspects of the project include examining recent crises, such as the Arab Spring and protests in Turkey, through "digital traces" on social media.[127] Tracking and analyzing sentiment and how social movements occur is an aspect of sentiment analysis technologies that may provide avenues with which to develop more detailed cybersurveillance of potential threats identified by the national security and intelligence communities.[128]

---

[115] *Id.* at A-2.

[116] *Id.* at A-5.

[117] Kessler, *supra* note 113.

[118] *See* Hu, *supra* note 26, at 138–39.

[119] *See, e.g.*, Gellman & Poitras, *supra* note 64 (describing one such instance).

[120] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801–1885c (2012)).

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

[122] *See, e.g.*, Ron Wyden, *Floor Statement on the Foreign Intelligence Surveillance Act (FISA)—June 25, 2008*, YOUTUBE (Jan. 15, 2009), https://www.youtube.com/watch?v=BgnO0s32Lvc.

[123] *See* Nafeez Ahmed, *Pentagon Preparing for Mass Civil Breakdown*, GUARDIAN (June 12, 2014, 2:00 EDT), https://www.theguardian.com/environment/earth-insight/2014/jun/12/pentagon-mass-civil-breakdown [https://perma.cc/3PCC-79JX].

[124] *Id.*

[125] MINERVA RES. INITIATIVE, http://minerva.defense.gov/ [https://perma.cc/F7AN-TLRS] (last visited Dec. 4, 2017).

[126] Ahmed, *supra* note 123.

[127] *Id.*

[128] *See id.*

Horizontal scaling and sentiment analysis programs appear in other branches of military research. The Office of Naval Research: Science and Technology (ONR) operates a program called the Human Social Cultural Behavioral Sciences Program (HSCB).[129] According to the ONR, HSCB "is a technology investment area that strives to support decision making and improve tactical warfighter training and mission rehearsal by developing cross-cultural and sociocultural skills, computational social science models and simulations."[130] The goals of the HSCB is to provide the Navy and Marine Corps with the ability "to identify, anticipate and defeat adaptive irregular threats operating within the physical, cyber and sociocultural domains."[131] Within the context of the DoD, the HSCB program has been described as a tool to serve intelligence ends.[132] According to the DoD, it is intended to provide the military "with the knowledge and tools to understand the dynamics of regional populations through the development of data collection and analysis methods, computational social science models and sociocultural training methods and tools."[133] HSCB, like other horizontal scanning programs, relies on big data "to develop, implement, and demonstrate forecasting and predictive models of human behavior for both analytic application and warfighter training."[134]

In addition to domestic horizontal scanning and cybersurveillance, the United States' cybersurveillance technology and philosophies have been exported. Singapore appears to have adopted a TIA-like program in the form of its Risk Assessment and Horizon Scanning (RAHS) program.[135] One of the consultants to RAHS, retired Navy Vice Admiral and former National Security Advisor John M. Poindexter, led TIA during its brief existence.[136] In an article for *Foreign Policy* detailing RAHS, Shane Harris explains that "Singapore is testing whether mass surveillance and big data can not only protect national security, but actually engineer a more harmonious society."[137] RAHS is a national defense program rooted in cybersurveillance tools.[138] Because RAHS appears to be TIA-inspired, and uses big data to strengthen national defense, it is unsurprising that the U.S. intelligence community has taken notice of

---

[129] *Human Social Cultural Behavioral Sciences*, OFF. NAVAL RES. (Oct. 2012), https://www.onr.navy.mil/en/Media-Center/Fact-Sheets/Human-Social-Cultural-Behavior [https://perma.cc/4YRA-7FM7].

[130] *Id.*

[131] *Id.*

[132] *See id.*

[133] *Id.*

[134] *Human, Social, Culture, & Behavior (HSCB) Modeling*, PAC. SCI. & ENGINEERING GROUP, http://www.pacific-science.com/ad7/sites/default/files/HSCB%20Project%20Summary_13Mar12_0pdf [https://perma.cc/DB69-QMQV] (last visited Dec. 4, 2017).

[135] Shane Harris, *The Social Laboratory*, FOREIGN POL'Y (July 29, 2014), http://www.foreignpolicy.com/2014/07/29/the-social-laboratory/ [https://perma.cc/J644-D6CV].

[136] *Id.* ("After Poindexter left DARPA in 2003, he became a consultant to RAHS, and many American spooks have traveled to Singapore to study the program firsthand.").

[137] *Id.*

[138] *See id.*

the Singapore model.[139] RAHS demonstrates a troubling future for big data cybersurveillance as more than just a tool of national security. RAHS appears to trace the path of the National Surveillance State: an administrative state that increasingly facilitates bureaucratized cybersurveillance.[140] RAHS's horizontal scanning capabilities are used for a multitude of functions: budgeting, economics, policymaking, and education plans, as well as broad sentiment analysis of the population.[141]

Horizontal cybersurveillance programs such as Social Radar, TIA, and RAHS signal how the National Surveillance State may be in the process of transforming into a National Cybersurveillance State. Horizontal scanning and geofencing tools have been utilized by U.S. law enforcement agencies,[142] and the long-term impact of such cybersurveillance, as well as its constitutional implications, are as yet unknown.

B. Basic Mechanics of Social Radar

Social Radar aims to engage in sentiment analysis, as well as to provide geographic and social tracking. Thus, Social Radar would permit a more active and targeted engagement with the population under analysis.[143] It would rely on data "to sense, if not forecast, a broad spectrum of phenomena (e.g., political, economic, social, environmental, health) and potentially forecast changing trends in population perceptions and behaviors."[144] Social Radar also was intended to provide a way to determine how individuals within the population would interact.[145] Such a tool would also be useful in counterinsurgency operations to track sentiment in the population and to determine the effectiveness or ineffectiveness of such actions.[146]

Social Radar appears to necessarily implicate big data tools: global, real-time data acquisition; capacity to process multiple forms of media; comprehending, recognizing, and understanding speech, images and video; automated and continuous communication analysis; geolocational analyses of social media platforms; and capacity to identify and track individual or group connections.[147] Social Radar would

---

[139] *See id.* ("[M]any current and former U.S. officials have come to see Singapore as a model for how they'd build an intelligence apparatus if privacy laws and a long tradition of civil liberties weren't standing in the way.").

[140] *See id.*

[141] *Id.*; *see also* Hu, *supra* note 26, at 144–45 (detailing RAHS and what the program is capable of).

[142] *See supra* notes 85–94 and accompanying text.

[143] *See* MAYBURY, *supra* note 105, at 3 ("*Social Radar* needs to sense perceptions, attitudes, beliefs and behaviors . . . and geographically and/or socially localize and track these to support the smart engagement of foreign populations and the assessment and replanning of efforts based on indicator progression.").

[144] *Id.*

[145] *Id.* ("[A] social radar should enable us to forecast who will cluster with whom in a network, where, and when in what kinds of relationships.").

[146] *See id.* at 6–7.

[147] *See id.* at 4–5.

appear to operate as a suspicionless form of surveillance—it would use "sources and methods that do not require active polling or engagement," and it would utilize anonymous collection methods to "help[ ] mitigate bias that is inevitable when the person/population is aware of the data collection."[148] The "architecture"[149] behind Social Radar includes the potential sources of information, such as military, legal, political, economic, social, health, and environmental data. Uses for Social Radar include: communication, counterinsurgency, and humanitarian methods.[150]

C. Current Status of Social Radar and Social Radar-Type Programs

Social Radar is under development by MITRE.[151] Another MITRE paper, published in 2012, explains that Social Radar would be useful "to understand, track, anticipate the effects of, or react effectively to the kinds of communication that feed large scale uprisings, or to understand and exploit the relationship between non-kinetic messaging and nation-state stability."[152] This paper noted the relationship between social media use and civil unrest in the Arab Spring, and pointed out that the communications on social media "play a very important part in building the networks that enable violent extremism, developing the strategies, tactics, and actions of violent extremist organizations, and determining the impact they have on adversaries and general populations."[153] Effective "[S]ocial [R]adar depends on continuous access to global data on general population perceptions, attitudes, opinions, sentiments, and behaviors."[154] The 2012 paper poses a number of questions that are essential to reach the ideal goals of Social Radar, including using mobile devices and crowd sourcing to "collect and process relevant social media and Internet data," and processing and analyzing data "at a global scale."[155] Sentiment analysis in Social Radar would need to include the ability to quickly determine public opinion, whether social media could be predictive, and determine how ideas, messages, and sentiment spread.[156]

---

[148] *Id.* at 4.

[149] *Id.* at 6–7. Experts increasingly describe dataveillance, big data surveillance, and cybersurveillance 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 [digital data collection and analysis] has evolved into a shockingly extensive, robust, and profitable surveillance architecture."); *see also* JENNIFER STISA GRANICK, AMERICAN SPIES: MODERN SURVEILLANCE, WHY YOU SHOULD CARE, AND WHAT TO DO ABOUT IT (2017); JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE (2004); Hu, *supra* note 54, at 1687, 1690, 1705.

[150] MAYBURY, *supra* note 105, at 7.

[151] *Id.* at 9.

[152] BARRY COSTA & JOHN BOINEY, MITRE CORP., SOCIAL RADAR 3-1–3-2 (2012), https://www.mitre.org/sites/default/files/pdf/12_0581.pdf [https://perma.cc/CR2V-JHHN].

[153] *Id.* at 3-2.

[154] *Id.* at 3-5.

[155] *Id.* at 3-6.

[156] *See id.* at 3-9–3-10.

Another paper, *Social Radar Workflows, Dashboards, and Environment*s,[157] deploys Social Radar to analyze, using Twitter access,[158] the 2011 United Kingdom riots and election protests.[159] Per the paper, Social Radar search tools include "Global Instability Hotspotting," "Sentiment Analysis," "Sensitive Instability Detectors and Emotion Analyses for Twitter," "Emotion Graphing," "Comment Filtering," "Topic Clouds," and "Course of Action Models."[160] According to this document, "[a] significant portion of the Social Radar data falls into the big data category, as it is composed of billions of small text messages."[161] The authors also note the potential uses for Social Radar in stability operations outside the United States,[162] counterinsurgency,[163] peacekeeping operations,[164] foreign internal defense,[165] foreign humanitarian assistance,[166] and combatting weapons of mass destruction.[167]

MITRE currently offers Social Radar Technologies for licensing.[168] According to MITRE, Social Radar "allow[s] analysts to detect, track, and understand social change in information-dense environments faster than humans alone are typically able."[169] Social Radar tools can process sources of information, such as news, tweets, and blogs for sentiment analysis, identifying influence developing "short-term forecasts, and support[ing] option analysis and decision making."[170] MITRE also claims

---

[157] JENNIFER MATHIEU ET AL., MITRE CORP., SOCIAL RADAR WORKFLOWS, DASHBOARDS, AND ENVIRONMENTS (2012), https://www.mitre.org/sites/default/files/pdf/12_0567.pdf [https://perma.cc/9B63-UP2S].

[158] *Id.* at 25-3.

[159] *Id.*

[160] *Id.* at 25-4–25-6.

[161] *Id.* at 25-14. The authors of this paper do not explain what they mean by the term "text messages."

[162] "Stability Operations occur outside of the US in coordination with other 'national powers to maintain or re-establish a safe and secure environment and to provide essential government services, emergency infrastructure reconstruction, and humanitarian relief.'" *Id.* at 25-20.

[163] "Counterinsurgency encompasses comprehensive civilian and military efforts taken to defeat an insurgency and address core grievances." *Id.* (internal quotations omitted).

[164] "A [p]eace [o]peration contains conflict, redresses the peace, and shapes the environment to support reconciliation and rebuilding, and facilitates the transition to legitimate governance." *Id.* (internal quotations omitted).

[165] "Foreign Internal Defense participates with civilian agencies in action taken by another government to free and protect its society from subversion, lawlessness, insurgency, terrorism, and other threats to its security . . . ." *Id.* (internal quotations omitted).

[166] "Foreign Humanitarian Assistance occurs outside of the US in coordination with the Department of State to relieve or reduce human suffering, disease, hunger, or privation." *Id.* (internal quotations omitted).

[167] "Combatting Weapons of Mass Destruction includes offensive operations against WMD, defensive operations, and managing the consequences of WMD attacks." *Id.* (internal quotations omitted).

[168] *Social Radar Technologies*, *supra* note 7.

[169] *Id.*

[170] *Id.*

that Social Radar tools can determine and measure sentiment; identify changes in sentiment; identify (1) key influencers, (2) who is engaged in the discussion, and (3) demographics of participants; determine which groups and organizations are manipulating social media and measure their influence; and evaluate courses of action for possible outcomes and effectiveness of actions.[171]

In 2015, MITRE "licensed its social analytics technologies to AtrocityWatch, a [non-]profit [organization] that uses big data to predict and prevent global atrocities."[172] AtrocityWatch is intending to use the technology to help "detect[ ] early warning signs of major events, such as genocide and war crimes, through crowd sourcing and data analytics."[173] Tools such as Social Radar may indeed be useful in tracking sentiment to prevent atrocity and violence. For example, during the 1994 Rwanda Genocide, increasingly violent propaganda was used to motivate Hutus to kill Tutsis.[174] Horizontal scanning sentiment analysis tools, however, also present the potential for abuse by military, intelligence, or law enforcement agencies. Because they often rely on publicly available data,[175] it is possible that such tools may not fall within the protections of the Fourth Amendment. However, the mass cybersurveillance of public opinion and ideas does raise both Fourth Amendment and First Amendment concerns.

CONCLUSION

Social Radar and other horizontal cybersurveillance technologies often rely on digital information that is made public or can be acquired through other means. Under the current Fourth Amendment jurisprudence, digitized data available at the government's disposal for analysis and preemptive decision-making may not be considered private. The question now posed by the challenges of horizontal cybersurveillance is whether indiscriminate mass surveillance that is population-wide is reasonable or consistent with constitutional values.

Specifically, the need to further intertwine the protections of both the First and Fourth Amendments is becoming more urgent. Emerging techniques of governing and policing are increasingly anchored in cybersurveillance technologies.[176] These technologies feed upon developments in big data, the Information Society, the Internet

---

[171] *See id.*

[172] Press Release, MITRE Corp., MITRE Licenses Social Radar Technology to AtrocityWatch (May 13, 2015), https://www.mitre.org/news/press-releases/mitre-licenses-social-radar-technology-to-atrocitywatch [https://perma.cc/BE6P-P457].

[173] *Id.*

[174] *See, e.g.*, David Yanagizawa-Drott, *Propaganda and Conflict: Evidence from the Rwandan Genocide*, 129 Q.J. ECON. 1947 (2014).

[175] *See* Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL'Y REV. 15, 33–38 (2016).

[176] *See* Paul Ohm, *Electronic Surveillance Law and the Intra-Agency Separation of Powers*, 47 U.S.F. L. REV. 269 (2012) (detailing how the U.S. is becoming a surveillance society).

of Things, and the Digital Economy. Social, political, and economic transformations track technological transformations.[177]

The new challenge is to determine what the constitutional response must be when the danger presented is constant surveillance and digital assessment. What if the threat is not to be silenced, detained, incarcerated? In a big data world, the threat flows from digital watchlisting, indiscriminate suspicionless cybersurveillance, data-basing, and algorithmic decision-making. The consequences of these threats are not just physical harms, but threats to free agency and natural rights. The byproduct of surveillance is a chilling effect to associational and expressive freedoms—in short, the loss of privacy that makes free thought and speech possible. The First and Fourth Amendments are, as the Supreme Court has acknowledged, intertwined,[178] thus a threat to one in the National Surveillance State may be a threat to the other. It is increasingly difficult to disentangle which rights are being infringed upon by horizontal cybersurveillance and data-driven policing practices.

In the past, surveillance arose in the context of criminal investigation and national domestic or foreign intelligence gathering. Now surveillance exists merely for the sake of surveillance—because the technological capacity exists. To preserve the fundamental democratic freedoms at the core of our Constitution, it is necessary to examine the relationship between the First and Fourth Amendments in light of modern cybersurveillance practices and to consider how that relationship may be used to guard against suspicionless intrusions.

---

[177] *See id.*

[178] *See, e.g.*, Zurcher v. Stanford Daily, 436 U.S. 547, 564–65, 567–68 (1978).