2017

Biometric Cyberintelligence and the Posse Comitatus Act

Margaret Hu
Washington and Lee University School of Law, hum@wlu.edu

BIOMETRIC CYBERINTELLIGENCE AND THE POSSE COMITATUS ACT

Margaret Hu[*]

ABSTRACT

This Article addresses the rapid growth of what the military and the intelligence community refer to as "biometric-enabled intelligence." This newly emerging intelligence tool is reliant upon biometric databases—for example, digitalized storage of scanned fingerprints and irises, digital photographs for facial recognition technology, and DNA. This Article introduces the term "biometric cyberintelligence" to more accurately describe the manner in which this new tool is dependent upon cybersurveillance and big data's mass-integrative systems.

This Article argues that the Posse Comitatus Act of 1878, designed to limit the deployment of federal military resources in the service of domestic policies, will be difficult to enforce to protect against militarized cyberpolicing and cybersurveillance harms that may generate from the domestic use of military grade cybersurveillance tools. Maintaining strict separation of data between military and intelligence operations on the one hand, and civilian, homeland security, and domestic law enforcement agencies on the other hand, is increasingly difficult as cooperative data sharing increases. The Posse Comitatus Act and constitutional protections such as the Fourth Amendment's privacy jurisprudence, therefore, must be reinforced in the digital age to appropriately protect citizens from militarized cyberpolicing: the blending of

---

[*] Margaret Hu, Associate Professor of Law, Washington and Lee University School of Law. My deepest gratitude to those who graciously offered comments on this draft, or who offered perspectives and expertise on this research through our thoughtful discussions: Sahar Aziz, Laurie Blank, Dorothy Brown, Mary Dudziak, Charlie Dunlap, Josh Fairfield, Amos Guiora, Rachel Levinson-Waldman, Erik Luna, Tim MacDonnell, Peter Margulies, Russ Miller, Steve Miskinis, Jeff Powell, Victoria Sahani, Shoba Wadhia, Ben Wittes, and apologies to those whom I may have inadvertently failed to acknowledge. In addition, this research benefited greatly from the discussions generated from the *Emory Law Journal*'s 2016 Thrower Symposium: *Redefined National Security Threats: Tensions and Legal Implications*, and the 2014 Symposium: *Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair*, co-hosted by the *German Law Journal* and the University of Freiburg, KORSE Centre for Security and Society in Freiburg, Germany. Many thanks to Nathan North, Editor in Chief; Jennifer Craig, Executive Managing Editor; and to the *Emory Law Journal* for their editorial care. Many thanks to the research assistance of Lauren Bugg, Russell Caleb Chaplain, Cadman Kiker, Alexandra L. Klein, and Kirby Kreider. All errors and omissions are my own.

military/foreign intelligence tools and operations, and homeland security/domestic law enforcement tools and operations. The Article concludes that, as of yet, neither statutory nor constitutional protections have evolved sufficiently to cover the unprecedented surveillance harms posed by the migration of biometric cyberintelligence from foreign to domestic use.

INTRODUCTION

The potential cybersurveillance consequences of mass biometric data collection are not yet fully known.[1] What is known, however, is that mass biometric data storage and analysis can lead to multiple unprecedented legal challenges[2] as big data tools and new forms of cybersurveillance technologies place increasing strain on existing privacy law doctrine,[3] statutory data privacy protections, and constitutional protections.[4] Experts note that this legal strain is

---

[1] Multiple scholars and experts have researched the legal consequences of newly emerging surveillance technologies, including those disclosed by former NSA contractor, Edward Snowden. *See, e.g.*, Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 162–64 (2015); Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 366–71 (2015); Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 498–500 (2015); Orin S. Kerr, *A Rule of Lenity for National Security Surveillance Law*, 100 VA. L. REV. 1513, 1515–18 (2014); Paul Ohm, *Electronic Surveillance Law and the Intra-Agency Separation of Powers*, 47 U.S.F. L. REV. 269, 287–89 (2012); Nathan Alexander Sales, *Domesticating Programmatic Surveillance: Some Thoughts on the NSA Controversy*, 10 I/S: J.L. & POL'Y FOR INFO. SOC'Y 523, 533–34 (2014); Margo Schlanger, *Intelligence Legalism and the National Security Agency's Civil Liberties Gap*, 6 HARV. NAT'L SECURITY J. 112, 117–19 (2015); 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, 725–28 (2014); Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721, 1723–24 (2014) [hereinafter Slobogin, *Panvasive Surveillance*]; Omer Tene, *A New Harm Matrix for Cybersecurity Surveillance*, 12 COLO. TECH. L.J. 391, 412–14 (2014); Patrick Toomey & Brett Max Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants, & the Right to Notice*, 54 SANTA CLARA L. REV. 843, 844–46 (2014); Stephen I. Vladeck, *Standing and Secret Surveillance*, 10 I/S: J.L. & POL'Y FOR INFO. SOC'Y 551, 554, 566–68 (2014); John Yoo, *The Legality of the National Security Agency's Bulk Data Surveillance Programs*, 37 HARV. J.L. & PUB. POL'Y 901, 901–07 (2014).

[2] *See, e.g.*, JENNIFER LYNCH, IMMIGRATION POL'Y CTR., FROM FINGER PRINTS TO DNA: BIOMETRIC DATA COLLECTION IN U.S. IMMIGRANT COMMUNITIES AND BEYOND 12–13 (2012); Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 551–53 (2012); D.H. Kaye, *Please, Let's Bury the Junk: The CODIS Loci and the Revelation of Private Information*, 102 NW. U. L. REV. COLLOQUY 70, 70–71 (2007); David H. Kaye, *Rounding Up the Usual Suspects: A Legal and Logical Analysis of DNA Trawling Cases*, 87 N.C. L. REV. 425, 426–33 (2009) (discussing how prosecutors can identify defendants by "trawling" through databases of DNA to generate random matches); Andrea Roth, *Safety in Numbers? Deciding When DNA Alone Is Enough to Convict*, 85 N.Y.U. L. REV. 1130, 1158–70 (2010); *see also* A. MICHAEL FROOMKIN & JONATHAN WEINBERG, CHIEF JUSTICE EARL WARREN INST. ON LAW & SOC. POLICY, HARD TO BELIEVE: THE HIGH COST OF A BIOMETRIC IDENTITY CARD 8–9 (2012), http://www.law.berkeley.edu/files/Believe_Report_Final.pdf.

[3] *See, e.g.*, CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 17 (2007); Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. F. 262, 265–66 (2013); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1956 (2013); Christopher Slobogin, *Is the Fourth Amendment Relevant in a Technological Age?*, *in* CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE 11, 12 (Jeffrey Rosen & Benjamin Wittes eds., 2011); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1136–37 (2002).

[4] *See, e.g.*, RACHEL LEVINSON-WALDMAN, BRENNAN CTR. FOR JUSTICE, WHAT THE GOVERNMENT DOES WITH AMERICANS' DATA 2–3 (2013); Fred H. Cate, *Government Data Mining: The Need for a Legal*

especially acute as the programmatic and technological architecture of big data cybersurveillance can be embedded within the data collection and data analysis protocols of civilian and domestic law enforcement activities,[5] and the everyday activities of an information society that is in the midst of a big data revolution.[6] Therefore, maintaining strict separation of data sharing between military and foreign intelligence operations[7] on the one hand, and civilian, homeland security, and domestic law enforcement agencies on the other hand,[8] is increasingly difficult and may be impracticable.

To better understand the potential legal consequences of the merger of civilian and military, along with domestic and foreign mass biometric data harvesting, this Article demonstrates the potential long-term cybersurveillance consequences of the increased sharing of biometric databases between military, intelligence, and law enforcement organizations, and other public and private entities.[9] Specifically, this Article contends that biometric cybersurveillance and biometric cyberintelligence objectives are increasingly used to justify the mass digital capture and analysis of unique physiological and behavioral traits of

---

Framework, 43 HARV. C.R.-C.L. L. REV. 435, 453 (2008); Jennifer C. Daskal, *Pre-Crime Restraints: The Explosion of Targeted, Noncustodial Prevention*, 99 CORNELL L. REV. 327, 353–54 (2014); Peter Margulies, *Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection After Snowden*, 66 HASTINGS L.J. 1, 51–52 (2014); Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 328–29 (2008); Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343, 349–50 (2008).

[5] *See, e.g.*, Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 103–04 (2014); Joshua A.T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981, 992 (2014); David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 101–03 (2013).

[6] *See, e.g.*, VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (2013); JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE 175–84 (2004); Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63, 65 (2012); *see also* DAVID LYON, THE ELECTRONIC EYE: THE RISE OF SURVEILLANCE SOCIETY 197 (1994); David Lyon, *Surveillance as Social Sorting: Computer Codes and Mobile Bodies*, *in* SURVEILLANCE AS SOCIAL SORTING: PRIVACY, RISK, AND DIGITAL DISCRIMINATION 13, 13 (David Lyon ed., 2003).

[7] *See, e.g.*, William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEX. L. REV. 1633, 1658 (2010); William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209, 1278–80 (2007).

[8] *See, e.g.*, Stephen I. Vladeck, *Big Data Before and After Snowden*, 7 J. NAT'L SECURITY L. & POL'Y 333, 334 (2014).

[9] Multiple scholars have researched the intersection of biometric identification technologies and post-9/11 government surveillance. *See, e.g.*, GLOBAL SURVEILLANCE AND POLICING: BORDERS, SECURITY, IDENTITY (Elia Zureik & Mark B. Salter eds., 2005); David Lyon, *Biometrics, Identification and Surveillance*, 22 BIOETHICS 499, 500 (2008); Erin Murphy, *Paradigms of Restraint*, 57 DUKE L.J. 1321, 1328–44 (2008); Lior Jacob Strahilevitz, *Signaling Exhaustion and Perfect Exclusion*, 10 J. ON TELECOMM. & HIGH TECH. L. 321, 326–27 (2012); Elia Zureik & Karen Hindle, *Governance, Security and Technology: The Case of Biometrics*, 73 STUD. POL. ECON. 113, 121–24 (2004).

entire populations and subpopulations.[10] Traditional bureaucratized surveillance protocols are in the process of merging with bureaucratized big data cybersurveillance systems to increasingly incentivize the development of universal biometric databases of the entire citizenry, often through biometric-based national ID systems,[11] and particular biometric databases of targeted classes within a specific citizenry, for example, DNA databases of arrestees.[12] Further, as nations enter into agreements to share biometric databases for military defense, foreign intelligence, and law enforcement purposes, the multinational cybersurveillance implications of biometric data collection and data analysis are likely to expand over time.[13]

Biometrics is "[t]he science of automatic identification or identity verification of individuals using physiological or behavioral characteristics."[14]

---

[10] *See, e.g.*, David H. Kaye, *A Fourth Amendment Theory for Arrestee DNA and Other Biometric Databases*, 15 U. PA. J. CONST. L. 1095, 1096–97 (2013); Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 CALIF. L. REV. 721, 725–26 (2007). Other scholars specifically focus their scholarship on a growing predominance of behavioral genetics and the use of neuroscience evidence in the criminal justice system. *See, e.g.*, Nita A. Farahany, *Incriminating Thoughts*, 64 STAN. L. REV. 351, 367–68 (2012); Nita A. Farahany, *Searching Secrets*, 160 U. PA. L. REV. 1239, 1241–42 (2012).

[11] For a discussion of what documents comprise identity cards and the surveillance consequences of identity documents, see generally DAVID LYON, IDENTIFYING CITIZENS: ID CARDS AS SURVEILLANCE (2009); PLAYING THE IDENTITY CARD: SURVEILLANCE, SECURITY AND IDENTIFICATION IN GLOBAL PERSPECTIVE (Colin J. Bennett & David Lyon eds., 2008). For an overview of the legal and policy implications of recently adopted and recently proposed digitalized identification systems, including privacy issues, see, for example, JIM HARPER, IDENTITY CRISIS: HOW IDENTIFICATION IS OVERUSED AND MISUNDERSTOOD 4–5 (2006); LAWRENCE LESSIG, CODE VERSION 2.0, at 45–54, 68–70 (2d ed. 2006); Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality: A Survey*, *in* PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION 15, 29 (Katherine J. Strandburg & Daniela Stan Raicu eds., 2006); Richard Sobel, *The Demeaning of Identity and Personhood in National Identification Systems*, 15 HARV. J.L. & TECH. 319, 323–24 (2002).

[12] *See, e.g.*, Elizabeth E. Joh, *DNA Theft: Recognizing the Crime of Nonconsensual Genetic Collection and Testing*, 91 B.U. L. REV. 665, 668–70 (2011); Erin Murphy, *License, Registration, Cheek Swab: DNA Testing and the Divided Court*, 127 HARV. L. REV. 161 (2013).

[13] *See, e.g.*, U.K. BORDER AGENCY, REPORT OF A PRIVACY IMPACT ASSESSMENT CONDUCTED BY THE UK BORDER AGENCY IN RELATION TO THE HIGH VALUE DATA SHARING PROTOCOL AMONGST THE IMMIGRATION AUTHORITIES OF THE FIVE COUNTRY CONFERENCE 34–35 (Dec. 9, 2010), http://www.ukba.homeoffice.gov.uk/sitecontent/documents/aboutus/workingwithus/high-value-data-sharing-protocol/pia.pdf.

[14] JOHN R. VACCA, BIOMETRIC TECHNOLOGIES AND VERIFICATION SYSTEMS 589 (2007). Numerous scholars and experts have explored the science and application of biometrics and the consequences of this emerging technology. *See, e.g.*, BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES (Joseph N. Pato & Lynette I. Millett eds., 2010); KELLY A. GATES, OUR BIOMETRIC FUTURE: FACIAL RECOGNITION TECHNOLOGY AND THE CULTURE OF SURVEILLANCE 26–27 (2011); ANIL K. JAIN, ARUN A. ROSS & KARTHIK NANDAKUMAR, INTRODUCTION TO BIOMETRICS 43–44 (2011); DAVID LYON, SURVEILLANCE STUDIES: AN OVERVIEW 118–36 (2007); SHOSHANA AMIELLE MAGNET, WHEN BIOMETRICS FAIL: GENDER, RACE, AND THE TECHNOLOGY OF IDENTITY (2011); ROBERT O'HARROW, JR., NO PLACE TO HIDE 157–89 (2005); VACCA, *supra*; Robin Feldman, *Considerations on the Emerging Implementation of Biometric Technology*, 25 HASTINGS

Traditionally, these physiological traits have included digitally scanned fingerprints, digital photo analysis through facial recognition technology, iris scans, and DNA.[15] Increasingly, physiological identifiers that can be digitally captured, stored, and analyzed include more experimental biometrics, including gait,[16] skeletal bone scans,[17] scars and tattoos,[18] ear shape[19] and eyebrow shape,[20] breathing rates,[21] and eye pupil dilation,[22] among other identifiers.

Understanding how the intelligence community and military branches may use biometric cybersurveillance tools and techniques—indeed, understanding biometric cybersurveillance itself—is crucial to the ongoing project amongst legal scholars of understanding the burgeoning "National Surveillance State."[23] This academic inquiry theorizes the necessary legal safeguards to protect civil liberties and democratic governance while allowing the surveillance necessary for national security to go forward. Military surveillance abroad is less restrained

---

COMM. & ENT. L.J. 653, 667–69 (2003); U.S. GEN. ACCOUNTING OFFICE, GAO-03-174, TECHNOLOGY ASSESSMENT: USING BIOMETRICS FOR BORDER SECURITY (2002), http://www.gao.gov/assets/160/157313.pdf.

15 *See, e.g.*, SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY 37–61 (2000) (describing the rise of biometrics and expansion of biometric databases).

16 *See, e.g.*, VACCA, *supra* note 14, at 32.

17 *See, e.g.*, Sara Gates, *Knee Scan Identification: MRIs May Be Better Way to ID Travelers, Study Suggests*, HUFFINGTON POST (Jan. 25, 2013, 12:36 PM), http://www.huffingtonpost.com/2013/01/25/kneecap-scans-identification-biometric-id_n_2543042.html; Mathew J. Schwartz, *Skeletal Scans Explored for Crime Fighting*, INFORMATIONWEEK (Aug. 26, 2010, 12:58 PM), http://www.informationweek.com/database/skeletal-scans-explored-for-crime-fighting/d/d-id/1091933?.

18 *See, e.g.*, *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System*, FBI (Sept. 2015), https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/interstate-photo-system. The media stored by the FBI's Next Generation Identification system includes photographs searchable by using facial recognition technology, as well as photographs of scars, distinct marks, and tattoos. *See Next Generation Identification (NGI)*, FBI, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi (last visited Nov. 10, 2016); *Privacy Impact Assessment Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) Biometric Interoperability*, FBI (Jan. 18, 2012), https://www.fbi.gov/services/records-management/foipa/privacy-impact-assessments/iafis-ngi-biometric-interoperability.

19 *See, e.g.*, VACCA, *supra* note 14, at 203–04.

20 *See, e.g.*, YUJIE DONG & DAMON L. WOODARD, EYEBROW SHAPE-BASED FEATURES FOR BIOMETRIC RECOGNITION AND GENDER CLASSIFICATION: A FEASIBILITY STUDY (2011).

21 *See, e.g.*, U.S. DEP'T OF HOMELAND SEC., DHS/S&T/PIA-012(A), PRIVACY IMPACT ASSESSMENT UPDATE FOR THE FUTURE ATTRIBUTE SCREENING TECHNOLOGY (FAST)/PASSIVE METHODS FOR PRECISION BEHAVIORAL SCREENING 5 (2011) [hereinafter PRIVACY IMPACT ASSESSMENT FOR FAST (2011)], https://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast-a.pdf.

22 *See, e.g.*, Pam Benson, *Will Airports Screen for Body Signals? Researchers Hope So*, CNN (Oct. 6, 2009, 9:15 PM), http://www.cnn.com/2009/TECH/10/06/security.screening/index.html?eref=onion#cnnSTCText.html.

23 *See* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 3–5 (2008); Jack M. Balkin & Sanford Levinson, *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 FORDHAM L. REV. 489, 489–90 (2006).

than the kinds of civilian surveillance allowed domestically; however, the efficiencies of cybersurveillance technologies being tested and implemented abroad can and likely will, in time, have application in serving domestic law enforcement objectives and homeland security intelligence purposes.

Digitalized biometric data now forms the basis for what the U.S. government terms "biometrically enabled intelligence"[24] or "biometric-enabled intelligence,"[25] apparently used interchangeably. In the intelligence and military use context, biometrically-enabled intelligence "provides an analytical baseline by resolving identities through high-confidence biometric matching and fusion with other sources of intelligence to positively identify the person in question."[26] Biometric-enabled intelligence, in other words, is presented as an "analytical baseline" that is defensive in nature. It is described as a method to protect U.S. national security interests by making the identities of potential criminals and terrorists more fully transparent. The creation of an "analytical baseline" comprised of multiple biometric data points and other biographic data purportedly enhances the ability of the government to identify potential enemies of the state through mass data collection and analysis.

This Article uses the term "biometric cyberintelligence" to more descriptively capture the process of converting digitalized biometric data into a product that informs tactical operations and actionable intelligence. This conversion process fuses together digitalized biometric matching tools—reliant upon vast biometric databases and sophisticated algorithmic methodologies to appropriately "match" an individual's physiological and behavioral traits with identifiable information stored in digitalized biometric and biographic databases—with other emerging dataveillance tools[27] and big data

---

[24] Ben Iannotta, *Biometrics: A New Intelligence Battlefield; Brings Tech Choices & Challenges*, FORTUNA'S CORNER (May 14, 2013), http://fortunascorner.com/2013/05/14/biometrics-a-new-intelligence-battlefield-brings-tech-choices-challenges/.

[25] David Pendall & Cal Sieg, *Biometric-Enabled Intelligence in Regional Command-East*, 72 JOINT FORCE Q., 1st Quarter 2014, at 69, 70, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-72/jfq-72_69-74_Pendall-Sieg.pdf?ver=2014-03-13-152414-890.

[26] Paul Moruza, *Intelligence Center Develops Biometrically Enabled Intelligence to Support Warfighter*, U.S. ARMY (Jan. 8, 2013), http://www.army.mil/article/93969/Intelligence_center_develops_Biometrically_Enabled_Intelligence_to_support_warfighter/ (quoting Cathy Moore, Senior Intelligence Analyst, U.S. Army, Biometrics Division, National Ground Intelligence Center).

[27] Data fusion has been described as "the collection of information from myriad sources to be organized and analyzed for a fuller picture of terrorist or other threats." DANA PRIEST & WILLIAM M. ARKIN, TOP SECRET AMERICA: THE RISE OF THE NEW AMERICAN SECURITY STATE 92 (2011). In the consumer context, "data fusion" has been defined in the following way: "Data fusion occurs when data from different sources are brought into contact and new facts emerge . . . ." PRESIDENT'S COUNCIL OF ADVISORS ON SCI. AND TECH., EXEC. OFFICE OF THE PRESIDENT, REPORT TO THE PRESIDENT: BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE, at x

cybersurveillance systems.[28] Whereas "biometric-enabled intelligence" appears to be a term that focuses more on the physiological or other forensic-based identification of potential criminal and terrorist suspects, this Article introduces the term "biometric cyberintelligence" to foreground the cybersurveillance consequences and intelligence-driven objectives of a data fusion process. More than just enabling a new kind of intelligence, biometric cyberintelligence is enabling a new kind of transformative policymaking protocol and governance philosophy, and needs to be grappled with constitutionally in that context.

Understanding this transformation necessitates contrasting how biometric data operated in a small data world versus how biometric data now operates in a big data world. In a small data world, traditionally, the linking of a potential criminal suspect or terrorist suspect to forensic evidence included the reliance upon biometric data such as fingerprints and DNA.[29] The newly emerging biometric analytic processes engaged by the military and the foreign and domestic intelligence community, however, increasingly utilize big data systems and data science tools rather than traditional small-data forensic science tools.[30] In a big data world, the data backbone for discerning the identity of a potential suspect or terrorist target, and the determination of whether consequences should attach to such identification, is increasingly an algorithmic process.[31] Therefore, emerging biometric-dependent intelligence tactics should be understood as uniquely cyber-centered and big data driven. This shift from small data biometric collection and analysis to big data biometric collection and analysis, particularly in military and intelligence operations and tactics, should also be understood as paradigmatic, likely to result in profound and lasting consequences.

(2014). Several scholars and experts have explored the legal and surveillance implications of data fusion centers that have been created by the government, particularly after the terrorist attacks of September 11, 2001. *See, e.g.*, PRIEST & ARKIN, *supra*, at 92–93; Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441 (2011); Slobogin, *Panvasive Surveillance*, *supra* note 1.

[28] *See, e.g.*, GATES, *supra* note 14, at 46–47; MAGNET, *supra* note 14; O'HARROW, *supra* note 14, at 157–89; Margaret Hu, *Biometric ID Cybersurveillance*, 88 IND. L.J. 1475, 1478–82 (2013) [hereinafter Hu, *Biometric ID*]; Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV. 773, 782–85 (2015) [hereinafter Hu, *Data Cybersurveillance*].

[29] *See, e.g.*, Iannotta, *supra* note 24.

[30] *See, e.g.*, Hu, *Data Cybersurveillance*, *supra* note 28, at 775–81.

[31] *See, e.g.*, James Risen & Laura Poitras, *N.S.A. Collecting Millions of Faces from Web Images*, N.Y. TIMES (May 31, 2014), http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html.

The potential cybersurveillance consequences of mass biometric data collection are increasingly apparent. For example, National Security Presidential Directive 59 and Homeland Security Presidential Directive 24 (NSPD-59/HSPD-24)[32] requires that data collection by military and civilian authorities be "interoperable"—that is, structured so that civilian data and military data can be commingled as needed.[33] NSPD-59/HSPD-24 in effect mandates a big data-driven bridge that makes feasible a link between military and foreign intelligence data gathering on one side, and domestic law enforcement and other civilian intelligence data gathering on the other side. The rationale for requiring interoperability of data collection across government is that it will make it easy to share data where various entities share common data tracking goals, but it is clear that the value of such efficiencies will undermine the firewall that Congress and the Constitution attempt to establish between such entities in other contexts.[34]

The phenomenon of biometric cyberintelligence cannot be understood without first explicating the underlying policy rationale for comprehensive biometric cybersurveillance generally. Further, it is important to recognize and describe the potential long-term National Surveillance State consequences of an increasing reliance on biometric data to serve a wide range of foreign and domestic security goals. Consequently, this Article is highly technical and descriptive. This descriptive effort, however, is necessary and critical. Understanding the legal implications of the emerging National Surveillance State requires a fuller understanding of the technologies and policy rationales that comprise the cybersurveillance architecture of the National Surveillance State. This Article, therefore, is a companion to earlier related works.[35] Like these related works, this Article must show the contours of the problem before addressing its legal implications.

Accordingly, this Article proceeds in three Parts. Part I contextualizes the commingling of data surveillance and cybersurveillance evidence between military, intelligence, and domestic law enforcement organizations. Part I begins

---

[32] Directive on Biometrics for Identification and Screening to Enhance National Security, NSPD-59/HSPD-24, 1 PUB. PAPERS 757 (June 5, 2008) [hereinafter Directive on Biometrics], https://www.gpo.gov/fdsys/pkg/PPP-2008-book1/pdf/PPP-2008-book1-doc-pg757.pdf ("This directive establishes a framework to ensure that Federal executive departments and agencies . . . use mutually compatible methods and procedures in the collection, storage, use, analysis, and sharing of biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner . . . .").

[33] *Id.* at 758.

[34] *See infra* notes 134–137, 333–335 and accompanying text.

[35] Hu, *Biometric ID*, *supra* note 28; Hu, *Data Cybersurveillance*, *supra* note 28.

with a brief overview of how the Snowden disclosures and recent criminal law cases combined shed light on how surveillance and big data cybersurveillance technologies deployed by the intelligence community can facilitate state and local law enforcement activities. Thus, these criminal cases illustrate the manner in which incriminating data, gathered either inadvertently or deliberately by intelligence activities, including data gathered in cybersurveillance sweeps of average civilians and non-terrorist targets, can be shared with domestic law enforcement and domestic intelligence agencies to enable prosecution.

Next, Part I presents a recent Ninth Circuit U.S. Court of Appeals case, *United States v. Dreyer*,[36] as a case study. *Dreyer* demonstrates exactly how military intelligence and cybersurveillance capacities typically deployed abroad for counterterrorism purposes can be deployed domestically for more day-to-day criminal law enforcement uses, for example, here, a child pornography investigation.[37]

Part II describes an increasing reliance by the military and intelligence community on biometric data and big data cybersurveillance systems to inform tactical decisionmaking. It focuses on how digitalized biometric data is increasingly collected in ways that are civilian-based and bureaucratized or routinized through day-to-day governance. In other words, the programmatic and technological architecture of biometric-enabled intelligence can be embedded in the data collection and data analysis protocols of civilian and domestic law enforcement activities. This Article argues that as biometric database sharing becomes more common, maintaining strict separation of data sharing between military and intelligence operations on the one hand, and civilian homeland security and domestic law enforcement agencies on the other hand, is increasingly difficult and may be impracticable.

Part III discusses how this conversion process—the process of gathering and analyzing biometric data and converting the data into cyberintelligence—can serve offensive rather than defensive goals. This discussion characterizes biometric cyberintelligence as an active operational movement by the military and intelligence community, situated within a coordinated cybersurveillance strategy, to comprehensively capture the biometric data and personally identifiable data of entire populations.[38] To demonstrate the potential lethality

---

[36] 767 F.3d 826 (9th Cir. 2014).

[37] *Id.* at 827–28.

[38] Drone strikes have been characterized in the media and elsewhere as an offensive and preemptive military strategy. *See, e.g.*, Andrew Callam, *Drone Wars: Armed Unmanned Aerial Vehicles*, 18 INT'L AFFAIRS

of the emerging technological and policy development of biometric cyberintelligence and biometric-enabled evidence, this Part illustrates how digitalized biometric data may be increasingly integrated into biometric drone weaponry and targeting drone strike technologies. This Part contends that the biometric cybersurveillance and biometric cyberintelligence technologies currently deployed abroad by the military and foreign intelligence communities are likely to migrate back to the homeland, and will likely be deployed domestically for federal and state law enforcement and security objectives.

Finally, the Article concludes that increasing bureaucratization of cybersurveillance generally, and biometric cybersurveillance in particular, is integral to the rapid growth of the National Surveillance State. Although biometric data has been traditionally limited to forensic evidence and small data identification purposes, it appears that biometric cyberintelligence objectives may now facilitate new forms of big data tracking and mass targeting, and may entail unknown consequences in the context of the National Surveillance State.[39] Yet, as witnessed in *Dreyer*, federal courts will likely struggle with how to apply the Posse Comitatus Act and constitutional protections such as the Fourth Amendment's privacy jurisprudence. *Dreyer* is a historic case in that it is an opportunity to question what legal tools, such as the Posse Comitatus Act, may be currently available to protect citizens from militarized cyberpolicing. The importance of this question is likely to increase as cyberintelligence tools are progressively integrated into daily law enforcement activities.

REV. (2010), http://www.iar-gwu.org/node/144 ("[T]he CIA primarily utilizes its Predator drones in the third type of operation: hunter-killer missions. These operations can extend U.S. offensive capabilities into areas in which the United States has little or no access."); Golo M. Bartsch, *Drones as a Means of a Pre-emptive Security Strategy*, ATLANTIC-COMMUNITY.ORG (Oct. 8, 2013), http://www.atlantic-community.org/-/drones-as-a-means-of-a-pre-emptive-security-strategy ("UCAVs [Unmanned Combat Aerial Vehicles] can literally be operated 'below the radar' in a political and societal sense . . . . This obviously makes UCAVs suitable weapons for governments pursuing a 'pre-emptive' security strategy."); Michael Hastings, *The Rise of the Killer Drones: How America Goes to War in Secret*, ROLLING STONE (Apr. 16, 2012), http://www.rollingstone.com/politics/news/the-rise-of-the-killer-drones-how-america-goes-to-war-in-secret-20120416 ("Obama's drone program, in fact, amounts to the largest unmanned aerial offensive ever conducted in military history . . . ."); Daniel Mabrey, *Unmanned Assassins: UAVs and the War on Terrorism*, 19 CRIME & JUST. INT'L (2003), http://www.cjimagazine.com/archives/cjif62c.html?id=36 ("[T]he Predator drones and other UAVs had never openly been used as offensive weapons prior to the military strikes in Afghanistan."). Others in the media and elsewhere have characterized drone strikes as defensive in nature. *See, e.g.*, Michael Gerson, *Obama's Drone Policy Is Rooted in Self-Defense*, WASH. POST (Feb. 7, 2013), https://www.washingtonpost.com/opinions/michael-gerson-obamas-drone-policy-is-rooted-in-self-defense/2013/02/06/4f1da2c2-708e-11e2-8b8d-e0b59a1b8e2a_story.html?utm_term=.c23166e99a02 ("Drone strikes are an innovation in anticipatory self-defense . . . .").

[39] Balkin, *supra* note 23, at 3–4; Balkin & Levinson, *supra* note 23, at 490, 528.

I. CYBERSURVEILLANCE, MILITARY-INTELLIGENCE DATA GATHERING, AND THE POSSE COMITATUS ACT

Recent media disclosures, including—most prominently—those of former NSA contractor Edward Snowden,[40] begin to reveal the extent to which the U.S. intelligence communities, both foreign and domestic, increasingly collects and stores digitalized biometric data.[41] More specifically, the Snowden disclosures reveal the increasing importance of biometric data as a component of mass surveillance and a critical tool in intelligence gathering. There is currently a rapid expansion of biometric databases among the intelligence community, the U.S. military,[42] and in the public and private sectors generally.[43] Biometric data is collected by various state and federal agencies for differing purposes in both the civilian and criminal context.[44] Additionally, the biometric data collection capacities and biometric-enabled technologies in the private sector—such as the replacement of traditional numeric passcodes with newly emerging biometric passcodes, including biometric verification on smartphones,[45] and other electronics and smart technologies[46]—have rapidly expanded in recent years as well.

In the aftermath of the terrorist attacks of September 11, 2001, the U.S. government has claimed that biometric data, particularly when combined with

---

[40] *See, e.g.*, GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE (2014).

[41] *See, e.g.*, Risen & Poitras, *supra* note 31 (stating that the Snowden disclosures revealed the NSA collects millions of digital photographs from Internet and social media sources and utilizes facial recognition technology to identify individuals); Stephanie Simon, *The Feds' Push for Big Data*, POLITICO (May 14, 2014, 5:09 AM), http://www.politico.com/story/2014/05/feds-big-data-106650.html (discussing Obama Administration initiatives seeking to "leverage the power of big data," including the building of an FBI facial recognition database to augment its fingerprint collection).

[42] *See, e.g.*, Rod Nordland, *Afghanistan Has Big Plans for Biometric Data*, N.Y. TIMES (Nov. 19, 2011), http://www.nytimes.com/2011/11/20/world/asia/in-afghanistan-big-plans-to-gather-biometric-data.html; Thom Shanker, *To Track Militants, U.S. Has System that Never Forgets a Face*, N.Y. TIMES (July 13, 2011), http://www.nytimes.com/2011/07/14/world/asia/14identity.html?_r=0.

[43] *See, e.g.*, GLOBAL SURVEILLANCE AND POLICING, *supra* note 9; *see also* Lyon, *supra* note 9, at 500; Murphy, *supra* note 9, at 1341–42; Zureik & Hindle, *supra* note 9, at 122.

[44] *See, e.g.*, Hu, *Biometric ID*, *supra* note 28, at 1476–83.

[45] *See, e.g.*, Jack Purcher, *Seven of Apple's Biometric Patents Surface Today Covering Touch ID for Online Commerce, Redacting Documents & More*, PATENTLY APPLE (Mar. 12, 2015, 10:39 AM), http://www.patentlyapple.com/patently-apple/2015/03/seven-of-apples-biometric-patents-surface-today-covering-touch-id-for-online-commerce-redacting-documents-more.html.

[46] *See, e.g.*, Ed Bott, *Microsoft to Add 'Enterprise Grade' Biometric Security to Windows 10*, ZDNET (Mar. 17, 2015, 9:04 AM), http://www.zdnet.com/article/microsoft-to-add-enterprise-grade-biometric-security-to-windows-10/ (announcing Microsoft's planned 2015 replacement of passwords with fingerprint and iris recognition in Windows 10 devices).

biographic and contextual data (e.g., behavioral data and pattern of life analytics), critically serves multiple national security and homeland security objectives.[47] For instance, in June 2008, President George W. Bush signed NSPD-59/HSPD-24.[48] With the implementation of NSPD-59/HSPD-24, it is federal policy that biometric data be collected in forms that can be readily shared with other federal agencies, and that such data be shared where a person is suspected of posing a threat to national security.[49] The U.S. Department of Defense is one of the agencies expressly subject to NSPD-59/HSPD-24,[50] and is, in fact, at the cutting edge of developing methods to collect and convert biometric data into actionable intelligence, as this Article details.[51]

The national cybersurveillance state has been documented elsewhere with a specific focus on the growing host of technologies and government programs associated with the capture and analysis of biometric data.[52] In this Article, I focus more specifically on the military capture and use of biometric data and the ways that it assists in the population management policies that are a component of current U.S. military operations abroad. These military efficiencies in biometric surveillance can—and do—have application at home.[53]

Jack Balkin[54] and Sanford Levinson[55] have theorized the emergence of a National Surveillance State that is an outgrowth of the national security state and the welfare state, itself their "logical successor."[56] The importance of thinking in terms of a National Surveillance State—rather than just an efflorescence of surveillance programs—is that it helps us to understand that surveillance is more

---

[47] The 9/11 Commission Report, for example, emphasized the need to incorporate biometric data into identity management tools and systems in order to augment border security and national security objectives. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., 9/11 COMMISSION REPORT 385–92 (2004), http://www.9-11commission.gov/report/911Report.pdf ("Linking biometric passports to good data systems and decisionmaking is a fundamental goal.").

[48] Directive on Biometrics, *supra* note 32.

[49] *Id.*

[50] *Id.* at 759. The Directive specifies the "Secretaries of State, Defense, and Homeland Security," as well as the Attorney General and the DNI, but also extends to include "the heads of other appropriate agencies," making its application across the federal government open-ended. *Id.*

[51] *See infra* Part III.

[52] *See, e.g.*, Hu, *Biometric ID*, *supra* note 28.

[53] *See, e.g.*, *infra* note 278.

[54] Knight Professor of Constitutional Law and the First Amendment, Yale Law School, and the founder and director of the Information Society Project, Yale Law School. *Jack M. Balkin*, YALE LAW SCH., https://www.law.yale.edu/jack-m-balkin (last visited Aug. 31, 2016).

[55] W. St. John Garwood and W. St. John Garwood, Jr. Centennial Chair in Law, University of Texas School of Law. *Sanford Levinson*, UNIV. OF TEX. SCH. OF LAW, https://law.utexas.edu/faculty/svl55/ (last visited Nov. 18, 2016).

[56] *See, e.g.*, Balkin, *supra* note 23, at 5.

than just about collecting and analyzing data for law enforcement purposes. Bureaucratized surveillance is about governing. Consequently, big data cybersurveillance tools currently being tested and deployed represent a new technique of governing—one that helps agencies outside purely law enforcement contexts to analyze and keep track of populations and population sub-groups. As big data cybersurveillance tools become more predictive in their ambition, the surveillance activities focus more on the tendencies of those populations and subgroups for the purpose of administering various national programs and for guiding public policy.[57]

Military surveillance of population biometrics abroad and understanding how it may facilitate military objectives provides more than a study in the cutting edge of surveillance techniques. It is also a study in techniques of governance available to the modern National Surveillance State, techniques whose efficiency will likely lead to support for their use at home.[58]

Before looking abroad, however, this Article turns first to two instances where military and foreign surveillance already has domestic impacts. Part I.A examines the phenomenon of "parallel construction." Parallel construction is the effort by domestic law enforcement to recreate intelligence transferred from outside agencies to mask the fact that such intelligence sharing is occurring. Part I.B looks at another instance of intelligence sharing as revealed by the Ninth Circuit case, *United States v. Dreyer*.[59] There naval investigators, although required by laws like the Posse Comitatus Act to restrict their law enforcement activities to military personnel, instead cast expansive surveillance nets—in the case at issue, encompassing the entire citizenry of the state of Washington.[60] The *Dreyer* case reveals that mass cybersurveillance does not easily abide distinctions like that between military and civilian or domestic and foreign intelligence. In *Dreyer*, naval surveillance was accomplished by monitoring all computers in the state of Washington to investigate naval personnel engaged in potential wrongdoing in that state.

---

[57] Balkin & Levinson, *supra* note 23, at 523 ("[A]lthough the transition to the National Surveillance State has been accelerated by the September 11 attacks and the Bush Administration's proclaimed War on Terror, its rise is overdetermined by a host of different technological and bureaucratic imperatives.").

[58] *See infra* note 275 and accompanying text.

[59] 767 F.3d 826 (9th Cir. 2014).

[60] *Id.* at 833–34.

A. "Parallel Construction": How Surveillance Data Is Shared Between Agencies and How Such Data Sharing Can Be Concealed

Recent revelations have demonstrated that intelligence agencies with different jurisdictions and purposes are sharing the results of their surveillance. This means, for example, that information gathered by the NSA that would be of interest to local law enforcement is passed to local law enforcement, which can then act on the surveillance by conducting an independent investigation and prosecution. This phenomenon has been brought to light by the recent scholarly work of Joshua Fairfield[61] and Erik Luna.[62] In *Digital Innocence*, Fairfield and Luna contend that the same big data tools that can be made available to the prosecution for evidence to incriminate the guilty should, conversely, be made available to the criminal defense for exculpatory evidence to exonerate the innocent.[63] This work documents the manner in which big data cybersurveillance technologies deployed by both foreign and domestic intelligence communities can facilitate federal, state, and local law enforcement activities.[64] It demonstrates that national surveillance programs justified on the basis of serving one objective, like national security, often are not limited to that objective, because incriminating data gathered inadvertently by intelligence activities against average civilians and non-terrorist targets can be shared domestically to enable state and federal prosecution.

Recently, in multiple domestic criminal cases in the U.S federal courts, the criminal defense discovered that the prosecution is relying upon classified evidence.[65] Often, the defense is made aware that incriminating evidence was

---

[61] Professor of Law at Washington and Lee University School of Law. *Joshua A.T. Fairfield*, WASH. & LEE UNIV. SCH. OF LAW, https://law2.wlu.edu/faculty/profiledetail.asp?id=242 (last visited Aug. 31, 2016).

[62] Amelia D. Lewis Professor of Constitutional and Criminal Law at Arizona State University's Sandra Day O'Connor College of Law. *Erik Luna*, ARIZ. STATE UNIV., https://apps.law.asu.edu/Apps/Faculty/Faculty.aspx?individual_id=127801 (last visited Nov. 17, 2016).

[63] Fairfield & Luna, *supra* note 5, at 1043–44.

[64] *Id.* at 996–1007.

[65] *See id.* at 1025 n.292 (citing United States v. Moalin, No. 10cr4246 JM, 2013 WL 6079518 (S.D. Cal. Nov. 18, 2013) (ordering that a new trial motion should be denied. This order also discusses the defendants motions to suppress FISA information and deny CIPA information)); *id.* at 1037 n.351 (citing United States v. Aref, 533 F.3d 72, 79–80 (2d Cir. 2008) (holding, inter alia, that as a matter of first impression, a motion to intervene to assert public's First Amendment right to access of criminal proceedings is proper)); *id.* at 1046 n.405 (citing United States v. Fernandez, 913 F.2d 148, 154 (4th Cir. 1990) (holding, inter alia, that there was no abuse of discretion in admission of certain information pertaining to certain intelligence projects and CIA locations that the Attorney General had stated were classified, where a district court judge had ruled them relevant and admissible)); *id.* at 1049 n.426 (citing United States v. Al-Arian, 267 F. Supp. 2d 1258, 1266 (M.D. Fla. 2003) (holding, among other things, that requiring defense attorneys and their staffs to submit to a security clearance procedure to protect classified information outweighed an individuals privacy interest)); *id.* at 1049

gathered against the criminal defendant pursuant to authorization under the Foreign Intelligence Surveillance Act (FISA) and authorized by the Foreign Intelligence Surveillance Court (FISA Court), or other classified evidence. FISA requires the government to obtain a judicial warrant similar to that required in criminal investigations prior to commencing intelligence-gathering operations within the United States.[66] Warrant applications submitted to the FISA Court are drafted by government attorneys and must include certification that the proposed surveillance is targeted against a foreign power or its agent.[67] In the case of inadvertent collection of information involving a U.S. citizen or resident alien, the government must minimize nonpublic information captured.[68] Where it has come to light that the prosecution is relying upon classified evidence, the defense must then seek access to the classified evidence by viewing the fruits of the cybersurveillance or the evidence of other secret intelligence activities—for example, the data or other evidence collected by the NSA and the CIA. In some of the cases identified, access to the classified evidence must be sought pursuant to the Classified Information Procedures Act (CIPA) of 1980.[69]

Intelligence agencies appear to disguise the sharing of surveillance information by encouraging or requiring the recipient agency of such surveillance data to engage in parallel construction.[70] Parallel construction occurs when law enforcement receives intelligence from the NSA or another secret intelligence source. Law enforcement officials reconstruct the evidence to hide the original source of the information (e.g., the data gathering activities of the NSA).[71]

---

n.427 (citing United States v. Abu Ali, 528 F.3d 210, 253–54 (4th Cir. 2008) (holding, among other things, that a district court's determination that redacted classified information need not be disclosed to the defendant, his uncleared counsel, and the public was not an abuse of discretion, and that the exclusion of the defendant and his counsel from proceedings related to this information was not violative of the Confrontation Clause)).

66 Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783.

67 50 U.S.C. § 1802(a) (2012).

68 *See* 50 U.S.C. § 1801(h) (2012).

69 Pub. L. No. 96–456, 94 Stat. 2025 (1980) (codified at 18 U.S.C. app. iii §§ 1–16 (2012)).

70 Fairfield & Luna, *supra* note 5, at 1042.

71 *Id.* at 1042–43. Fairfield and Luna elaborate:

> [I]ntelligence and law enforcement agencies have actively shared information. Reportedly, however, law enforcement officials have been instructed to hide the source of this information. According to documents reviewed by the news agency Reuters, an entity within the Drug Enforcement Agency—the Special Operations Division (SOD)—funnels NSA intelligence to law enforcement officers but directs them to conceal the true origins of any resulting criminal investigation from defense attorneys, prosecutors, and judges. To pull off this ruse, law enforcement is trained to 'recreate' information through a process euphemistically termed 'parallel

In other words, parallel construction recreates legitimate domestic law enforcement evidence from foreign intelligence or secret intelligence.[72] This deliberate reconstruction of evidence, in effect, covers up the fact that such secret intelligence sharing occurred. The data sharing between the secret intelligence agency with the domestic law enforcement agency may be covered up out of concerns about the legality of the sharing of such information, or concerns about unwanted disclosure. Either way, the broader consequences constitutional are profound. In effect, surveillance capacities authorized for the purpose of protecting the domestic population from foreign threats are being turned upon that very population and used against it, even if that is not the primary purpose of such surveillance.

If military or foreign intelligence gathered by governmental agencies ostensibly not concerned with enforcement of domestic laws is secretly used for that purpose, then this is the very hallmark of the National Surveillance State, according to Balkin and Levinson.[73] Further, Balkin and Levinson predict that under the National Surveillance State, secret law enforcement systems that at first are kept separate from transparent law enforcement systems will eventually intersect.[74] Parallel construction appears to signal that at the earliest stages of the National Surveillance State, we are witnessing the merger between the secret law enforcement system and the transparent law enforcement system.

B. Posse Comitatus Act and United States v. Dreyer

Data sharing of surveillance results also occurs between military agencies and civilian agencies—even though there are legal protections designed to inhibit such transfers, as illustrated by recent cybersurveillance and data sharing case, *United States v. Dreyer*.[75] *Dreyer* concerned mass cybersurveillance technology that had been deployed by Naval intelligence domestically. The cybersurveillance was conducted to uncover military personnel engaged in the traffic of child pornography, but the program cast a much wider net, placing all computers in the state of Washington under surveillance.[76]

---

construction': laundering the information in question by concocting independent sources through field interviews, confidential informants, physical searches and seizures, etc.

Id. at 1042 (footnotes omitted).

72 *Id.* at 1042.

73 *See* Balkin & Levinson, *supra* note 23, at 520–26.

74 *Id.*

75 767 F.3d 826 (9th Cir. 2014).

76 *Id.* at 833–34.

Generally, the Posse Comitatus Act (PCA) prohibits the Army and the Air Force from participating in the enforcement of civilian laws.[77] More specifically, the PCA prevents the personnel of the Army or Air Force from enforcing civilian laws without express constitutional or congressional authority.[78] By a separate statute, Congress required the Secretary of Defense to establish comparable regulations also preventing members of the Navy and Marine Corps from participating in civilian law enforcement.[79] Thus, the language of the PCA is often interpreted to extend to the Navy and Marines through U.S. Department of Defense policy.[80] The Act has led to exclusion of evidence, dismissal of criminal charges, and civil causes of action.[81] It is a criminal statute and can therefore "render[] the transgressor liable to criminal penalties."[82]

Most commonly, a violation of the PCA occurs when the military either performs tasks assigned to civil government or when the military performs tasks assigned to it for solely civilian government purposes.[83] Further, if the military provides assistance to civilian police, it cannot be direct. Though there are some

---

77 *See* 18 U.S.C. § 1385 (2012).

78 CHARLES DOYLE & JENNIFER K. ELSEA, CONG. RESEARCH SERV., R42659, THE POSSE COMITATUS ACT AND RELATED MATTERS: THE USE OF THE MILITARY TO EXECUTE CIVILIAN LAW, at Summary (2012), http://www.fas.org/sgp/crs/natsec/R42659.pdf.

79 10 U.S.C. § 375 (2012) ("The Secretary of Defense shall prescribe such regulations as may be necessary to ensure that any activity (including the provision of any equipment or facility or the assignment or detail of any personnel) under this chapter does not include or permit direct participation by a member of the Army, Navy, Air Force, or Marine Corps in a search, seizure, arrest, or other similar activity unless participation in such activity by such member is otherwise authorized by law."); *see also* 32 C.F.R. § 182.6(a)(1)(iii)(A) (2016) ("DoD personnel are prohibited from providing the following forms of direct civilian law enforcement assistance (1) Interdiction of a vehicle, vessel, aircraft, or other similar activity. (2) A search or seizure. (3) An arrest; apprehension; stop and frisk; engaging in interviews, interrogation, canvassing, or questioning of potential witnesses or suspects; or similar activity. (4) Using force or physical violence, brandishing a weapon, discharging or using a weapon, or threatening to discharge or use a weapon except in self-defense, in defense of other DoD persons in the vicinity, or in defense of non-DoD persons, including civilian law enforcement personnel, in the vicinity when directly related to an assigned activity or mission. (5) Evidence collection; security functions; crowd and traffic control; and operating, manning, or staffing checkpoints. (6) Surveillance or pursuit of individuals, vehicles, items, transactions, or physical locations, or acting as undercover agents, informants, investigators, or interrogators. (7) Forensic investigations or other testing of evidence obtained from a suspect for use in a civilian law enforcement investigation in the United States unless there is a DoD nexus (e.g., the victim is a member of the Military Services or the crime occurred on an installation under exclusive DoD jurisdiction) or the responsible civilian law enforcement official requesting such testing declares in writing that the evidence to be examined was obtained by consent. Requests for exceptions to this restriction must be made through channels to the ASD (HD&ASA), who will evaluate, in coordination with the General Counsel of the Department of Defense, whether to seek Secretary of Defense authorization for an exception to policy.")

80 DOYLE & ELSEA, *supra* note 78, at 56 n.332.

81 *Id.* at 62–65.

82 *E.g.*, United States v. Walden, 490 F.2d 372, 376 (4th Cir. 1974).

83 DOYLE & ELSEA, *supra* note 78, at 53.

exceptions,[84] there is direct assistance when military involvement: includes "'the exercise of regulatory, proscriptive, or compulsory military power'; . . . 'amount[s] to direct active involvement in the execution of the laws'; and . . . 'pervade[s] the activities of the civilian authorities.'"[85] Although the PCA mentions only the Army and the Air Force, courts have applied PCA-like rules to the Navy and Marines through other laws and administrative regulations.[86]

In *United States v. Dreye*r, the Ninth Circuit, sitting en banc, found that naval cybersurveillance of a state-wide scope violated the PCA and indicated that evidence resulting from future comparable violations could be subject to application of the exclusionary rule. Although the case did not involve direct surveillance of biometric data, it illustrates how cyberintelligence refuses to abide the bright line distinctions that Congress attempted to secure in statutes like the PCA.

Due to the litigation record, *Dreyer* provides a glimpse into how military cybersurveillance can easily result in direct consequences for civilians. The facts of the case tell a story about how military domestic surveillance resulted in local law enforcement actions against a civilian and private citizen. The case involves the use of a surveillance program referred to as "RoundUp" by Steve Logan, a special agent of the Brunswick, Georgia, office of the Naval Criminal Investigative Service (NCIS).[87] RoundUp made it possible to search all "computers located in Washington state sharing known child pornography on the Gnutella file-sharing network."[88] RoundUp identifies files that the user inputs "by comparing the 'SHA–1 hash values' of files being offered for download—unique identifiers that do not change when a file name is altered—with values already known to be associated with child pornography."[89] Through the RoundUp cybersurveillance software, it appears that the agent had the ability to search the file as well as determine who had downloaded the file through the file-sharing website.[90] Once the computer that downloaded it had been

---

[84] One exception is for an "independent military purpose," where the primary purpose of military participation is to "further[] a military or foreign affairs function . . . regardless of incidental benefits to civilian authorities." United States v. Dreyer, 767 F.3d 826, 833 (9th Cir. 2014), *abrogated by* 804 F.3d 1266 (9th Cir. 2015) (en banc) (quoting United States v. Hitchcock, 286 F.3d 1064 , 1069 (9th Cir. 2002)).

[85] *Dreyer*, 804 F.3d at 1275 (quoting United States v. Khan, 35 F.3d 426, 431 (9th Cir. 1994)).

[86] *Id.* at 1273 (explaining that "'PCA-like restrictions' adopted pursuant to § 375 apply to the Navy and NCIS . . . .").

[87] *Id.* at 1270.

[88] *Dreyer*, 767 F.3d at 827–28.

[89] *Id.* at 828 n.2.

[90] *Id.* at 828.

identified, the agent was able to download the files from that computer and verify the files contained child pornography.[91]

Logan "found a computer [on the Gnutella network] using the Internet Protocol (IP) address 67.160.77.21 sharing several files identified by RoundUp as child pornography."[92]After Logan searched the files and identified the computer that had downloaded the files in question, he made a request for an administrative subpoena for the name and address associated with the IP address.[93] This subpoena was then forwarded to the FBI, who, in turn, made an administrative subpoena request to Comcast.[94] Comcast then provided the name and address of the defendant, Michael Dreyer, pursuant to the administrative subpoena.[95] After Logan received the name and address of Dreyer from Comcast, verifying Dreyer as the user of the computer that had downloaded the files, Logan screened the U.S. Department of Defense database to determine if the defendant had a military affiliation.[96]

When Logan discovered that Dreyer had no current military affiliation, he wrote a report summarizing the incriminating evidence against Dreyer.[97] At this point, Logan submitted the report to the Washington state NCIS office.[98] That office gave the report and supporting material to local law enforcement authorities, namely Officer Schrimpsher of the Algona Police Department in the state of Washington.[99] Officer Schrimpsher contacted the Seattle, Washington, police department and received a sample of a search warrant affidavit.[100] Officer Schrimpsher then prepared a search warrant application, attached all of the materials given to him by Agent Logan, and filed it with the state court.[101] With the warrant, the Algona Police Department searched Dreyer's premises, found evidence of child pornography on his desktop computer, and confiscated it.[102] Dreyer was arrested and charged with distribution and possession of child pornography.[103] The cybersurveillance activities of Agent Logan were obtained

---

91 *Id.*
92 *Id.*
93 *Id.*
94 *Id.*
95 *Id.*
96 *Id.*
97 *Id.*
98 *Id.*
99 *Id.*
100 *Id.*
101 *Id.*
102 *Id.* at 828–29.
103 *Id.* at 829.

in discovery.[104] Dreyer was ultimately convicted. He appealed, arguing, among other things, the evidence should have been suppressed because his prosecution amounted to military enforcement of civilian laws in violation of the PCA-like restrictions applicable to the Navy.[105] Because the PCA does not expressly apply to Navy personnel, Dreyer argued that the NCIS involvement in his case violated PCA principles.[106] Even though NCIS agents, including Agent Logan, are civilians, the Ninth Circuit agreed that they acted under the auspices of the military.[107] The court further found that Logan was directly and actively involved in civilian enforcement in his role as an investigator.[108] That conduct violated Department of Defense regulations and policies placing the Navy under PCA-like restrictions, as required by 10 U.S.C. § 375.[109]

The initial Ninth Circuit panel held that evidence resulting from violations of the PCA-like restrictions on the Navy should be suppressed.[110] Although one judge dissented and at a rehearing en banc the application of the exclusionary rule was overturned, the reasons for initially applying the rule resulted from the panel's strong concerns about allowing such sweeping cybersurveillance to go unchecked. In the panel decision, the court explained that application of the exclusionary rule in the PCA context was only warranted where there exists a need to deter future violations.[111] The initial panel found a need for deterrence, having been struck by "the extraordinary nature of the surveillance": "So far as we can tell from the record, it has become a routine practice for the Navy to conduct surveillance of all the civilian computers in an entire state . . . ."[112] The decision suggests that the court was more concerned with the all-encompassing nature of the surveillance employed than with the fact that it was carried out under military auspices.

---

104 Schrimpsher's affidavit "contained a number of misrepresentations and omissions." Defendant-Appellant's Opening Brief at 8, United States v. Dreyer, 767 F.3d 826 (9th Cir. 2014) (No. 13-30077). "The government conceded that the warrant contained misrepresentations, but argued they were not fatal to the warrant because Schrimpsher appended Logan's report to his affidavit." *Id.* at 10.

105 *Dreyer*, 767 F.3d at 829–30 (discussing the Posse Comitatus Act, 18 U.S.C. § 1385 (2012)).

106 *Id.* PCA principles "apply to the Navy as a matter of Department of Defense . . . policy. *Id.* at 830.

107 *Id.* at 836–37.

108 *Id.* at 832. Courts have held that the following activities "constitute[d] an active role in direct law enforcement . . . : arrest; seizure of evidence; search of a person; search of a building; investigation of crime; interviewing witnesses; pursuit of an escaped civilian prisoner; search of an area for a suspect and other like activities." *See, e.g.*, United States v. Red Feather, 392 F. Supp. 916, 925 (D.S.D. 1975).

109 *Dreyer*, 767 F.3d at 830, 835.

110 *Id.* at 837.

111 *Id.* at 835–36.

112 *Id.* at 836.

Dreyer was later reheard by the Ninth Circuit en banc with the en banc decision departing from the panel decision in significant ways. While it upheld the finding that the surveillance was carried out in violation of the PCA-like restrictions applicable to the Navy, the en banc court concluded that suppression was not warranted in this instance, even though it reserved the possibility that suppression of evidence could be a remedy for future, comparable violations.[113] Here it is important to note how the cybersurveillance side of the biometric cybersurveillance coin shows that technological capacity outstrips attempts to create firewalls between military and civilian, and foreign and domestic operations. Logan engaged in a state-wide surveillance to target naval personnel engaged in sharing child pornography. His cybersurveillance search was found to be overbroad, casting the net too widely for the sake of efficiency, rather than trying to identify how to confine the initial search only to computers used by military personnel. After having identified suspects state-wide, the search was then narrowed to comport with the PCA by winnowing out non-military personnel—something the Ninth Circuit indicated should have been done in the first instance.

The panel decision noted that Agent Logan's activities may have fallen under the independent military purpose exception had he restricted his search to areas where there was a significant Navy interest rather than expanding it to all computers within the state of Washington.[114] Thus, the scope of the initial search brought it outside the reach of an independent military purpose. The court went further and noted that RoundUp displays the general geographic location of each hit—a suspect computer IP address.[115] Dreyer's IP address was located in an area within thirty miles of several military institutions—but that area also was close to Seattle and Tacoma, leading the panel to conclude again that there was insufficient evidence of a military purpose at this stage.[116]

Importantly, the violation of the PCA-like restrictions on the Navy derived then not from the fact that the NCIS agent passed the information he uncovered on to civilian authorities, but, from the scope of the surveillance itself.[117] The court rejected the government's view that such a search, without more, is acceptable, analogizing the NCIS's conduct to having NCIS agents "routinely

---

113 United States v. Dreyer, 804 F.3d 1266, 1280–81 (9th Cir. 2015) (en banc).

114 *Dreyer*, 767 F.3d at 833–34.

115 *Id.* at 834.

116 *Id.*

117 "Because Agent Logan's investigation itself violated the PCA-like restrictions, it is irrelevant whether it was permissible for him to transfer to civilian authorities" the unearthed information. *Id.* at 833 n.11.

stop suspected drunk drivers in downtown Seattle on the off-chance that a driver is a member of the military."[118]

After finding that PCA-like restrictions were violated, the court next had to decide whether evidence resulting from the violation should have been excluded. The panel noted that, typically, an exclusionary rule is not applied except where a "need to deter future violations is demonstrated."[119] The court found such a need here based on evidence that "it has become a routine practice for the Navy to conduct surveillance of all the civilian computers in an entire state to see whether any child pornography can be found on them."[120]

Judge Diarmuid O'Scannlain concurred in finding that the Navy's PCA-like restrictions had been violated, but dissented with regard to applying the exclusionary rule.[121] He emphasized that the remedy is generally disfavored because it can result in the release of an otherwise convicted criminal.[122] The dissent noted that application of the rule in the context of the PCA was unprecedented for any federal court and was particularly disturbing given that the criminal who would benefit was engaged in child pornography.[123]

Application of the exclusionary rule in the context of the PCA is only warranted where there is evidence of "widespread and repeated violations," and absent its application, future violations will not be deterred.[124] The dissent found such evidence lacking, noting that it amounted to "anecdotal evidence" that "four agents committed violations—three of whom were part of the same investigative team."[125] In contrast to the dissent's opposition to the application of the exclusionary rule to benefit a criminal involved with child pornography, Judge Andrew Kleinfeld joined the court's opinion and then concurred separately to expand upon the egregious nature of the government's conduct: through its surveillance, the military "peeked into every computer in the State" in what amounted to "repeated invasions of Washingtonians' privacy."[126]

---

118 *Id.* at 834.

119 *Id.* at 839 (quoting United States v. Roberts, 779 F.2d 565, 568 (9th Cir. 1986)).

120 *Id.* at 836.

121 *Id.* at 842 (O'Scannlain, J., concurring in part and dissenting in part).

122 *Id.* at 839 (O'Scannlain, J., concurring in part and dissenting in part) ("The rule's 'bottom-line effect, in many cases, is to suppress the truth and set the criminal loose in the community without punishment.'" (quoting Davis v. United States, 564 U.S. 229, 237 (2011))).

123 *Id.* at 838, 840.

124 *Id.* at 836–37.

125 *Id.* at 841 (O'Scannlain, J., concurring in part and dissenting in part).

126 *Id.* at 837–38 (Kleinfeld, J., concurring).

In other words, it seems likely the panel result was driven more by the court's concern about the state-wide surveillance undertaken than by the threat of military intrusion upon civilian affairs. The court, after all, did not reach the question of whether it was improper for the NCIS to pass information gleaned about private citizens to the civilian authorities. The conduct requiring deterrence was the use of a computer program that allowed law enforcement to, as Judge Kleinfeld put it, "hack[]" computers state-wide.[127]

The dissent, expressing strong disapproval over the cost of the deterrence—potentially freeing someone trafficking in child pornography and thus potentially aiding the victimization of children—further underscores the drastic nature of the court's action. Judge Kleinfeld's concurrence, however, rejoins to point out not only that the military, through such searches, is effectually "acting as a national police force,"[128] but also that there is a widespread invasion of privacy at issue here—an issue that is really separate from the concern that the military is overstepping the bounds Congress set for it.[129]

The en banc Ninth Circuit differed from the panel in terms of whether the exclusionary remedy was warranted but in important respects affirmed key aspects of the panel decision as relates to cybersurveillance. The court again found Logan had violated PCA-like restrictions on the Navy and again located the source of that violation in terms of the initial search, which because "the computer query employed . . . was in no way limited members of the military."[130] In other words "the methodology NCIS employed . . . clearly violated" the PCA-like restrictions on the Navy.[131]

The en banc court was more cautious about whether the violations were widespread and in the end attributed them to "institutional confusion" about what the PCA-like restrictions on the Navy required.[132] That in turn would allow the court to conclude suppression was not warranted since, the court reasoned, the Government should be given an opportunity to "self-correct" and conform to the law before application of such a harsh rule.[133]

---

127 *Id.* at 838.
128 *Id.* at 837.
129 *Id.*
130 United States v. Dreyer, 804 F.3d 1266, 1276 (9th Cir. 2015) (en banc).
131 *Id.*
132 *Id.*
133 *Id.* at 1280.

The decision was not a victory for either Dreyer or the government, and reflects the original panel's concern with cybersurveillance. In challenging the panel's resort to the exclusionary rule, the government argued, and the court agreed, that application of the exclusionary rule is normally restricted to deterring constitutional violations or violations of statutes enforcing constitutional norms.[134] The Ninth Circuit, however, then held that the PCA was a statute grounded in the Constitution.[135] The court did not identify a specific amendment to justify this. But, rather, the courts discovered its constitutional basis in a general structural argument. The court relied upon the constitutional separation of the military and civilian spheres, citing to a Supreme Court case which identified the Third Amendment's prohibition on quartering troops in civilian homes as reflecting a broader desire to preclude military intrusion (specifically military surveillance) on civilian activities.[136]

The result of *Dreyer* is that the Ninth Circuit reserved the right to invoke the exclusionary rule and preserved the remedy of excluding evidence resulting from military computer monitoring in the future. Moreover, pragmatically speaking, by declining to suppress evidence on the facts before it, the court insulated a potentially shaky holding that the PCA (and therefore the Navy's PCA-like restrictions) have constitutional underpinnings. As disturbing as the sweeping nature of military cybersurveillance was to the panel and the en banc court, the panel dissent made clear that allowing someone involved in child pornography to go free was equally disturbing—and such bad facts could potentially lead to unfavorable Supreme Court review.[137]

In *Dreyer*, the PCA-like restrictions applicable to the Navy provided the Ninth Circuit with the legal hook it needed to curb the Navy's state-wide surveillance. However, neither *Dreyer* nor the PCA prevent the same kind of surveillance from being undertaken by civilian authorities. Moreover, the PCA will not stop comparable programs from migrating from foreign military to domestic law enforcement use. Domestic applications may be put into play by civilian authorities asserting that these surveillance programs offer governing efficiencies that make them worthwhile. Yet, the legal framework to limit them and their potential intrusion of constitutional rights and privacy in general remains in need of being theorized.

---

134 *Id.* at 1277–78.

135 *Id.* at 1279.

136 *Id.* at 1279 n.7 (quoting Laird v. Tatum, 408 U.S. 1, 15 (1972)).

137 United States v. Dreyer, 767 F.3d 826, 840–41 (9th Cir. 2014) (O'Scannlain, J., concurring in part and dissenting in part).

As seen in *Dreyer*, with the tools of cybersurveillance at his disposal, a Naval intelligence agent deployed those tools against all citizens in an entire state. With cybersurveillance, surveillance is not designed to pursue and monitor suspects but rather to unearth them in the first place, separating them out from the general populace. Thus, in the case of RoundUp, the general populace of an entire geographic area, here the State of Washington, was subjected to cybersurveillance. Increasingly, according to the theorizing of Balkin and Levinson, traditional "rule of law" protocols will follow the secret law protocols of the National Surveillance State.[138] Thus, the kind of efficiency at play in *Dreyer* is precisely why the military's surveillance programs abroad deserve the attention of scholars.

The *Dreyer* illustration does not involve a biometric database with a biometric anchor. Rather, the anchor in that case was an IP address. That fact, however, does not diminish *Dreyer's* illustrative value, as local law enforcement officers may have been tasked with collecting the defendant's biometrics pursuant to procedure.[139] At the time of Dreyer's arrest, biometric data (e.g., fingerprints and digital photo) may have been harvested under normal law enforcement protocols, which often require sharing local biometric databases with federal law enforcement and homeland security agencies.

Additionally, Washington State mandates DNA collection for individuals convicted of certain felony sexual offenses, including being required to register as a sex offender.[140] Members of the Washington legislature have attempted to extend this law to encompass all felony arrestees since 2011.[141] All state databanks can be used for law enforcement officials investigating sex crimes.[142] The FBI maintains a national DNA database, "containing the DNA profiles contributed by federal, state, and local participating forensic laboratories."[143] In sum, a civilian, such as Dreyer, who was not intended to be the target of the intelligence gathering, may nonetheless find himself ensnared in the architecture

---

138 *See, e.g.*, Balkin, *supra* note 23, at 4–5.

139 *Dreyer*, 767 F.3d at 828.

140 *See* WASH. REV. CODE § 43.43.754 (2015) (identifying crimes triggering DNA collection, the collection procedure, and penalties for noncompliance).

141 *See* Deborah Wang, *Supreme Court Decision Revives Washington State Debate over DNA Collection*, KUOW.ORG (June 4, 2013), http://kuow.org/post/supreme-court-decision-revives-washington-state-debate-over-dna-collection.

142 Michelle Hibbert, *DNA Databanks: Law Enforcement's Greatest Surveillance Tool?*, 34 WAKE FOREST L. REV. 767, 780 (1999).

143 *Frequently Asked Questions on CODIS and NDIS*, FBI, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet (last visited Oct. 10, 2016).

of biometric cybersurveillance, by virtue of his data being potentially indefinitely stored in the databases of FBI and Department of Homeland Security (DHS), and perhaps the databases of other intelligence agencies—regardless of the final disposition of his case.

II. BIOMETRIC CYBERINTELLIGENCE

It is not readily apparent how the military and intelligence communities convert biometric-enabled intelligence into actionable intelligence through mass biometric cybersurveillance, nor is it obvious how biometric data can be exploited for drone weaponry and other targeted killing technologies. It is apparent, however, that biometric data is being actively collected. According to one report, in fact, "[t]he stated goal of the Afghan [biometric data collection] effort is no less than the collection of biometric data for every living person in Afghanistan."[144]

According to a 2012 report by the U.S. Government Accountability Office, "[i]n Afghanistan, the U.S. military is using more than 7,000 electronic devices to collect biometrics data in the form of fingerprints, iris scans, and facial photographs."[145] Additionally, "[f]rom 2004 to 2011, U.S. military forces collected biometrics data in the form of over 1.6 million [biometric] enrollments involving more than 1.1 million persons in Afghanistan, and used biometrics to successfully identify approximately 3,000 known enemy combatants."[146]

This Part explicates to what end is served by biometric-enabled intelligence. In Part II.A, the biometric cyberintelligence process is explained as beginning with the collection of biometric data and proceeds with its fusion with "contextual" data also collected from the target population. The result is actionable intelligence. Although biometric-enabled intelligence is often characterized by the military and intelligence community as the familiar and routinized collection of biometric data, such as fingerprints and DNA, to enhance identity information analysis (e.g., a fingerprint or DNA database to facilitate the government's attempt to identify a potential criminal suspect or terrorist), private contractor proponents are more enthusiastic about its potential.

---

144 *Identity Dominance: The U.S. Military's Biometric War in Afghanistan*, PUB. INTELLIGENCE (Apr. 21, 2014) [hereinafter *Identity Dominance*], https://publicintelligence.net/identity-dominance/.

145 U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-442, DEFENSE BIOMETRICS: ADDITIONAL TRAINING FOR LEADERS AND MORE TIMELY TRANSMISSION OF DATA COULD ENHANCE THE USE OF BIOMETRICS IN AFGHANISTAN 1 (2012), http://www.gao.gov/assets/600/590311.pdf.

146 *Id.* (footnote omitted).

To that end, this Part summarizes in detail the potential of biometric-enabled intelligence as portrayed by Booz Allen Hamilton, a government contractor on the forefront of biometric surveillance tactics and techniques.

The new forms of mass biometric data collection and analysis are unfolding at the dawn of a big data world. The biometric-driven forms of identity verification and determination now deployed in the civil, criminal, military, and intelligence contexts, therefore, are uniquely cyber-driven as these sectors attempt to harness the promise of newly emerging big data tools. Further, the collection of biometric data by the military and intelligence communities does not lead to static storage, as in a small data context (e.g., collection of fingerprint files in paper form and storing such files in filing cabinets). In the big data context, the storage and subsequent analysis of biometric data, including the linkage of biometric identifiers with other database screening and pattern analysis under data analytics, can lead to military and intelligence decisionmaking.

Domestically, these techniques are often referred to under the rubric of "identity management." In the context of military operations abroad, they are characterized as "population management." Part II.B discusses both. It focuses on how biometric data collection and analysis are increasingly executed through biometric National ID systems. Part II.C briefly considers the most aggressive aim of biometric-enabled intelligence: "identity dominance." Part II.D explains that identity dominance through identity management and population management incentivizes the burgeoning of interoperable biometric databases and bureaucracies attempting to coordinate biometric cybersurveillance and biometric cyberintelligence strategies.

A. Identity Intelligence and Biometric-Enabled Intelligence

At the time of the NSA surveillance disclosures, it was revealed that Edward Snowden was employed as a contractor for the NSA at a private corporation, Booz Allen Hamilton,[147] which refers to itself as a "strategy and technology consulting" firm.[148] Booz Allen describes itself as "a leading provider of

[147] Marjorie Censer, *Booz CEO: Snowden 'Was Not a Booz Allen Person'*, WASH. POST (July 31, 2013), http://www.washingtonpost.com/business/capitalbusiness/booz-ceo-snowden-was-not-a-booz-allen-person/2013/07/31/a349b51a-f9f6-11e2-8752-b41d7ed1f685_story.html. Censer explains, "Booz Allen, which is majority-owned by private equity firm Carlyle Group, was thrust into the spotlight after Snowden acknowledged being the source of news reports about National Security Agency data-collection programs." *Id.*

[148] *Booz Allen at a Glance*, BOOZ ALLEN HAMILTON, http://investors.boozallen.com/glance.cfm (last visited Aug. 18, 2016).

management consulting, technology, and engineering services to the U.S. government in defense, intelligence, and civil markets."[149] As a contractor seeking business with U.S. intelligence agencies, Booz Allen does what the military and other branches typically will not: pitches the way biometric intelligence can be put to proactive and preemptive uses.[150]

To better understand "identity intelligence" and "biometric-enabled intelligence," as terms of art in the defense and intelligence community vernacular, the Booz Allen website is informative. Booz Allen features a promotional page titled, "Identity/Biometrics Enabled Intelligence."[151] In another promotional publication, Booz Allen includes references to biometric and forensic identification technologies.[152] Booz Allen describes this identity intelligence as "authoritative information [that] adds a powerful new evidentiary source that can drive intelligence estimates and predictions."[153] According to Booz Allen, this process involves the full integration of biometrics "into the traditional intelligence analysis cycle," allowing for "raw biometric information" to be "fused with contextual information to produce useful and actionable intelligence."[154]

The Booz Allen description is consistent with the official policy of the U.S. Department of Defense, which also emphasizes the need to integrate biometrics and forensics into intelligence activities in order to support "the full range of military operations."[155] "BEI [biometric-enabled intelligence] and FEI [forensic-enabled intelligence] shall be fully integrated into Defense Intelligence and the Defense Intelligence Component activities as an essential element of

---

149 *Id.*

150 *See, e.g.*, Grey Burkhart, *Predictive Intelligence: The Critical Connection Between Intentions and Capabilities*, BOOZ ALLEN HAMILTON, http://www.boozallen.com/insights/2013/04/predictive-intelligence-the-critical-connection-between-intentions-and-capabilities (last visited Oct. 27, 2016) ("Predictive intelligence is one critical component of a holistic cybersecurity strategy that encompasses all the people, process, and technology facets of a dynamic defense posture to anticipate, prioritize, and mitigate cyber threats.").

151 *Identity/Biometrics Enabled Intelligence*, BOOZ ALLEN HAMILTON (Jan. 30, 2015) (on file with the author).

152 *Next-Generation Biometrics and Forensics: Moving Biometrics to the Tactical Edge*, BOOZ ALLEN HAMILTON, http://www.boozallen.com/content/dam/boozallen/media/file/next-generation-biometrics-and-forensics.pdf (last visited Nov. 13, 2016).

153 *Identity/Biometrics Enabled Intelligence*, *supra* note 151.

154 *Id.*

155 U.S. DEP'T OF DEF., INSTRUCTION NO. O-3300.04, DEFENSE BIOMETRIC ENABLED INTELLIGENCE (BEI) AND FORENSIC ENABLED INTELLIGENCE (FEI) 2 (2012), https://publicintelligence.net/dod-biometric-intelligence.

national security and in support of the full range of military operations consistent with national, defense, and operational priorities."[156]

Booz Allen's full description of "identity intelligence" is as follows:

> When biometrics and forensics are fully integrated with other intelligence disciplines and the intelligence analysis process, this authoritative identity information adds a powerful new evidentiary source that can drive intelligence estimates, predictions, and products. To turn disparate pieces of biometric data into meaningful analytics and substantive intelligence, raw biometric data (e.g., fingerprints, face images, iris & retina scans, voice signals, 3D full-body scans, latent forensic data, video & multimedia signals, among other data) is fused with other raw intelligence and contextual information to produce useful and actionable intelligence products. In a well-governed biometric-enabled intelligence organization, well-trained analysts use biometric case management tools, enterprise-class infrastructure, proven tools and techniques, and established processes to support mission-critical activities.[157]

Before biometric data can support intelligence analytics, a number of steps must occur. The biometric data must first be collected, and then it must be fused with broader contextual data about the biography of individuals based on their data trails. Booz Allen discusses the end product of this process, "biometric-enabled intelligence," in the following manner:

> Biometric Enabled intelligence has quickly become an accepted tool for solving high-priority identity problems. Biometric information exhibits an inherent reliability, whether it is collected overtly or covertly. Biometric identity data is readily indexed, processed, and retrieved. Intelligence analysts and law enforcement personnel use it as the central criteria to establish identity and as a basis to recommend action.[158]

In other words, biometric-enabled intelligence provides more than a library of data to be consulted after a crime has occurred. When fused with contextual information, it allows intelligence agencies to become proactive—to make appropriate interventions based on predictive analytics. Booz Allen further explains the objectives of biometric-enabled intelligence: "Intelligence

---

156 *Id.*

157 *Identity/Biometrics Enabled Intelligence*, *supra* note 151.

158 *Id.*

Communities use biometric-enabled intelligence in new strategic and tactical applications to proactively exploit biometric & forensic data[:]"

- "Can a person be matched to a place, activity or device?"[159]
- "Can faces in the crowd be linked to other intelligence information?"[160]
- "Can persons, objects, or other entities be linked?"[161]
- "Is the presence of multiple people in the same location an event of interest?"[162]
- "Can movement patterns b[e] anticipated exploited?"[163]
- "Can we predict the intent of a person or organization?"[164]
- "How does biometric and identity intelligence impact our strategic execution?"[165]

Booz Allen also offers an array of tactics, techniques, and tools that can be deployed to "exploit the rich potential of biometric-enabled intelligence[:]"[166]

- "Searching, analyzing, and mining biometric, identity, and forensic information";[167]
- "Using biometrics to create and enhance intelligence products";[168]
- "Implementing enterprise-class infrastructure to store and process biometric intelligence";[169]
- "Using biometric and identity linkages to establish attribution and identify risks";[170]

---

159 *Id.*
160 *Id.*
161 *Id.*
162 *Id.*
163 *Id.*
164 *Id.*
165 *Id.*
166 *Id.*
167 *Id.*
168 *Id.*
169 *Id.*
170 *Id.*

- "Identifying patterns in biometric and identity data";[171]
- "Supporting social and relational network analysis of criminal/terrorist/insurgent/foreign country intelligence networks";[172]
- "Communicating threats in real time";[173]
- "Tracking, monitoring, and cleansing identity information";[174]
- "Implementing novel biometric recognition technology to solve urgent and challenging ID problems";[175]
- "Integrating off-the-shelf technologies to create highly functional enterprise infrastructure";[176]
- "Building in-house biometric/identity expertise";[177]
- "Sharing biometric and identity data with customers and stakeholders";[178]
- "Creating new tactics, techniques, tools, processes, and standards";[179]
- "Applying techniques and analytics to identity-enabled intelligences."[180]

To better understand how Booz Allen is able to translate "raw biometric data" into, as they term it, "useful and actionable intelligence," it is important to ask exactly how "raw biometric data" is "fused with . . . contextual information."[181] Booz Allen explains that it possesses the capacity to "synthesize information from multiple . . . intelligence sources."[182]

---

171 *Id.*
172 *Id.*
173 *Id.*
174 *Id.*
175 *Id.*
176 *Id.*
177 *Id.*
178 *Id.*
179 *Id.*
180 *Id.*
181 *Id.*
182 *Id.* Booz Allen describes its methodology in full as follows:

> Booz Allen applies an intelligence perspective to the challenges of protection mitigation. Rather than focus on narrow, biometric-specific identification technologies, our methodology delivers the ability to define the value of disparate biometrics based on match quality and source reliability to

In the identity-management technology vernacular, "contextual information" is both very specific and very ambiguous. It is specific because it is seeking biographical information and information that detects individual characteristics (e.g., specific product preferences and Internet behavior patterns) that can form the basis of an accurate personal data profile. It is ambiguous because it is universal in nature and can involve the capture of limitless categories of biometric, biographical, and behavioral data.

The rise of the Internet in the 1990s allowed for more sophisticated research into the profiling of individuals as consumers of products (e.g., online purchases) and users of technology (e.g., Internet browsing) through the development of methods, tools, and techniques for "context in Information Access, Seeking and Retrieval," and evaluation.[183] Through complex algorithms that attempt to account for idiosyncratic anomalies and other factors of scientific instability (e.g., the reliability of data may be environment-dependent), daily advances in screening technologies have resulted in attempts to capture and then predict consumer tastes and technological user preferences and habits with more and more accuracy. Contextual information relies on the "access, seeking and retrieval" of biographical and informational choice data that can be obtained from the Internet, social-networking site activity, cell phones, GPS devices, personal databases, and publicly-available government databases.[184] In lay terms, contextual information can include:

> extract biometric-derived information as it applies to a unique mission. It also allows us to synthesize information from multiple intelligence sources to deliver to our clients the specific information they want and the certainty that they need.

Id.

[183] *CIRSE 2009: ECIR 2009 Workshop on Contextual Information Access, Seeking and Retrieval Evaluation*, WIKICFP (Apr. 6, 2009) http://www.wikicfp.com/cfp/servlet/event.showcfp?eventid=4394&copyownerid=320; *see also, e.g.*, MAYER-SCHÖNBERGER & CUKIER, *supra* note 6. The President's Council of Advisors on Science and Technology states:

> Individually, each data source may have a specific, limited purpose. Their combination, however, may uncover new meanings. In particular, data fusion can result in the identification of individual people, the creation of profiles of an individual, and the tracking of an individual's activities. More broadly, data analytics discovers patterns and correlations in large corpuses of data, using increasingly powerful statistical algorithms. If those data include personal data, the inferences flowing from data analytics may then be mapped back to inferences, both certain and uncertain, about individuals.

PRESIDENT'S COUNCIL OF ADVISORS ON SCI. AND TECH., *supra* note 27, at x; *see also* Azin Ashkan et al., *Classifying and Categorizing Query Intent*, *in* ADVANCES IN INFORMATION RETRIEVAL: 31TH EUROPEAN CONFERENCE ON IR RESEARCH, ECIR 2009, at 578, 578 (Mohand Boughanem et al. eds., 2009).

[184] Ms. Smith, *Microsoft's Davis on Privacy: Your Digital Life Data Is Bankable Currency*, NETWORK WORLD (Sept. 1, 2010, 6:06 AM), http://www.networkworld.com/community/node/65750.

> all locations that you go, all the purchases you ever make, all your relationships, all activity, all your health, governmental, employer, academic and financial records, your web search history, your calendars and appointments, all your phone calls, data, texts, email, all peoples connected to your social circle, all your personal interests, and all other personal data.[185]

In one study, for example, contextual information allowed for the construction of a profile of an Internet user based on "user context."[186] By conducting a "semantic [word context] analysis" of all files accessed over the Internet, the experts sought to "construct an ontological user profile describing the users preferences based on the users context."[187] The software is then programmed to adapt the individual's profile ontologically, or sort data based on the data's and the user's relationships with other data and other users with shared characteristics.[188] The profile grows in its sophistication in ever greater degrees of predictive value through correlative evidence over a period of time, continuing to study Internet activity and other technological "log files" that are added to the profile over the years and comparing it with other reliable comparator data and users.[189] Based on technological advances, therefore, the predictive analytics involving identity determinations can be made more accurate by not only comparing current behavioral patterns to prior behavioral patterns, but to others that are considered to be fair or similarly situated comparators within a target's profile,[190] including physiological and biometric information, which in turn includes "soft" biometric information (e.g., race, gender, skin color, etc.).

This fusion of data and, more specifically, the synthesis of biometric data with "contextual information," unfolds within a legal and administrative

---

185 *Id.* (discussing Partner Architect Marc Davis, Microsoft, Keynote Address at the Privacy Identity Innovation Conference (Aug. 18, 2010), https://vimeo.com/14401407 ("[A]ll the searches [you] do on Google or Bing or Yahoo, all the purchases [you] do on [your] credit cards, Amazon, [your] social graph on Facebook, Twitter, LinkedIn, [your] address book and [your] call logs, . . . [your] interests, expressed explicitly and implicitly, where [you] have been [and] plan to go, [your] calendar, and the list goes on and on.")).

186 Nazimuddin Mohammed, Trong Hai Duong & Geun Sik Jo, *Contextual Information Search Based on Ontological User Profile*, *in* COMPUTATIONAL COLLECTIVE INTELLIGENCE: TECHONOLOGIES AND APPLICATIONS, PART II 490, 491 (Jeng Shyang-Pan, Shyi-Ming Chen & Ngoc Thanh Nguyen eds., 2010).

187 *Id.* at 490; *see also id.* at 491 ("The ontological approach is a proven technique to model users and context in the field of information retrieval. . . . A new ontology can be created to represent a user's general information, such as name, age, birth date, educational background, to more specific information describing the user's interests.").

188 *Id.* at 491–92.

189 *Id.*

190 *Id.*

architecture that supports it. For example, after the terrorist attacks of September 11, 2001, and throughout his presidency, President George W. Bush signed several dozen executive orders titled as "Homeland Security Presidential Directives" (HSPDs) or "National Security Presidential Directives" (NSPDs). Multiple presidential directives relate to biometric screening technology either implicitly or explicitly, such as HSPD-6,[191] HSPD-11,[192] HSPD-12,[193] and NSPD-59/HSPD-24.[194] HSPD-6 is titled "Integration and Use of Screening Information to Protect Against Terrorism," and was signed by President Bush on September 16, 2003.[195] HSPD-11 is titled "Comprehensive Terrorist-Related Screening Procedures" and was signed by President Bush on August 27, 2004.[196] HSPD-11 is complimented by HSPD-12, titled "Policy for a Common Identification Standard for Federal Employees and Contractors."[197] HSPD-12 was signed by President Bush on the same date as HSPD-11, August 27, 2004.[198] HSPD-12 specifies a policy for the issuance of a standard digitalized biometric identification card for federal employees and contractors.[199] Implementing standards call for interoperable fingerprints to be used for interagency biometric verification purposes and permits federal agencies to utilize other biometrics for own-employee verification.[200]

---

191 Directive on Integration and Use of Screening Information to Protect Against Terrorism, HSPD-6, 2 PUB. PAPERS 1174 (Sept. 16, 2003) [hereinafter Directive on Integration and Use], https://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1174.pdf ("It is the policy of the United States to (1) develop, integrate, and maintain thorough, accurate, and current information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (Terrorist Information) . . . .").

192 Comprehensive Terrorist-Related Screening Procedures, HSPD-11, 2 PUB. PAPERS 1763 (Aug. 27, 2004), https://www.gpo.gov/fdsys/pkg/PPP-2004-book2/pdf/PPP-2004-book2-doc-pg1763.pdf ("[I]t is the policy of the United States to: (a) enhance terrorist-related screening . . . through comprehensive, coordinated procedures that detect, identify, track, and interdict people, cargo, conveyances, and other entities and objects that pose a threat to homeland security . . . .").

193 Policy for a Common Identification Standard for Federal Employees and Contractors, HSPD-12, 2 PUB. PAPERS 1765 (Aug. 27, 2004) [hereinafter Policy for a Common Identification Standard], https://www.gpo.gov/fdsys/pkg/WCPD-2004-08-30/pdf/WCPD-2004-08-30-Pg1709.pdf ("[I]t is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).").

194 Directive on Biometrics, *supra* note 32.

195 Directive on Integration and Use, *supra* note 191.

196 Comprehensive Terrorist-Related Screening Procedures, *supra* note 192.

197 Policy for a Common Identification Standard, *supra* note 193.

198 *Id.*

199 *Id.*

200 Implementation of HSPD-12 was promulgated through Federal Information Processing Standard 201 by the U.S. Department of Commerce National Institute of Standards and Technology (NIST), which detailed guidelines for Personal Identity Verification (PIV) credentials. U.S. OFFICE OF PERSONNEL MGMT., HSPD-12—

Perhaps most relevant to this Article, and as mentioned briefly in the Introduction, is a joint National Security Presidential Directive and Homeland Security Presidential Directive signed by President George W. Bush on June 5, 2008.[201] Titled "Biometrics for Identification and Screening to Enhance National Security," NSPD-59/HSPD-24 directs the military and federal government to work collaboratively "to collect, store, use, analyze, and share biometrics to identify and screen KSTs [known and suspected terrorists]."[202] NSPD-59/HSPD-24 also directs the military and federal government "to collect, store, use, analyze, and share biometrics" of "other persons."[203] No further guidance is provided on how to limit this instruction beyond the mandate that the collection, storage, use, analysis, and sharing of biometrics should be directed against those "who may pose a threat to national security."[204] Further, NSPD-59/HSPD-24 directs the executive branch to gather "biometric and associated biographic and contextual information of individuals in a lawful and appropriate manner, while respecting . . . privacy and other legal rights under United States law."[205]

NSPD-59/HSPD-24 appears to build upon existing identity-screening consolidation and coordination efforts put in motion by HSPD-6, HSPD-11, and HSPD-12. Specifically, it was intended to ensure that high-level identity screening programs are implemented throughout government.[206] This directive does not impose biometric or database screening requirements on state, local, or tribal authorities, or on the private sector. The directive does, however, provide a policy justification and legal rationale for the collection, retention, or dissemination of personal information for identification and screening activities.

ADVANCED FINGERPRINT RESULTS, NOTICE NO. 06-04 (June 8, 2006), https://www.opm.gov/investigations/background-investigations/federal-investigations-notices/2006/fin06-04.pdf. "On August 5, 2005, the Office of Management and Budget (OMB) issued Memorandum M-05-24 'Implementation of [HSPD] 12—Policy for a Common Identification Standard for Federal Employees and Contractors' . . . . In March 2006, NIST issued FIPS 201-1, 'Personal Identity Verification (PIV) of Federal Employees and Contractors' . . . ." *Id.* These guidelines identify a fingerprint-based background check as the bare minimum for a PIV credential. *Id.* For technical information about the implementation of HSPD-12, see *About Personal Identity Verification (PIV) of Federal Employees and Contractors*, NAT'L INST. STANDARDS & TECH., http://csrc.nist.gov/groups/SNS/piv/ (last updated Aug. 16, 2016).

201 Directive on Biometrics, *supra* note 32.

202 *Id.*

203 *Id.*

204 *Id.*

205 *Id.*

206 *Id.* at 757–60.

And, as noted above, Official U.S. Department of Defense policy on biometric cyberintelligence requires the fusion of "BEI and FEI with associated contextual data and other available intelligence."[207] It appears from the guidance that the "contextual data and other available intelligence" may include intelligence gathered through the NSA.[208] Specifically, the U.S. Department of Defense specifies multiple categories of available intelligence to be fused with biometric data: "[1] document and media exploitation, [2] signals intelligence (SIGINT), [3] human intelligence (HUMINT) . . . , and [4] counter human network operations that include counterterrorism, counterinsurgency, counterproliferation, counternarcotics, counterpiracy, and countersmuggling."[209]

Yet, experts agree that biometric use for military and intelligence decisionmaking is still a new field that relies upon experimental technologies.[210] "The general field or trade of identity intelligence . . . is in its infancy . . . ."[211] There are few guidelines that can assist in the verification of the reliability of biometrics and biometric-enabled intelligence. In fact, "the 2011 U.S. Army Commander's Guide to Biometrics in Afghanistan states that there is 'no formal doctrine; universally accepted tactics, techniques, and procedures; or institutionalized training programs across the Department of Defense' for biometric capabilities."[212]

"Many gaps exist in our understanding of the nature and extent of distinctiveness and stability of biometric traits across individuals and groups."[213] Experts caution that biometric technologies have not been tested for minimum efficacy levels when scaled to the volume of millions or billions of

---

207 U.S. DEP'T OF DEF., *supra* note 155, at 2.

208 *Id.*

209 *Id.* The Department of Defense instructs that these types of intelligence should "support irregular warfare (IW) in accordance with [DoD policy] . . . ." *Id.*

210 GARFINKEL, *supra* note 15, at 55 ("Despite their apparent accuracy, neither fingerprints nor DNA samples are suitable for identifying individuals on a day-to-day basis."); U.S. GEN. ACCOUNTING OFFICE, GAO-03-174, TECHNOLOGY ASSESSMENT: USING BIOMETRICS FOR BORDER SECURITY 58–62 (2002), http://www.gao.gov/assets/160/157313.pdf (explaining the "[l]ack of [a]pplications-[d]ependent [e]valuations" that study the impact of biometric data usage in real-life contexts and summarizing studies showing "[s]usceptibility [of biometric technologies] to [d]eception"). In contrast, the usage of biometric data for forensic purposes has undergone more rigorous and lengthier testing, having been tested over several decades. *See, e.g.*, GARFINKEL, *supra* note 15, at 59 (asserting that biometric recognition and verification technologies have not been subjected to the same scientific peer review process as that required of DNA fingerprinting).

211 Iannotta, *supra* note 24.

212 *Identity Dominance*, *supra* note 144.

213 BIOMETRIC RECOGNITION, *supra* note 14, at 4.

individuals.[214] "While biometric technology is currently available and is used in a variety of applications, questions remain regarding the technical and operational effectiveness of biometric technologies in large-scale applications."[215]

Although of only anecdotal value, for example, when reporting on Biometric-Enabled Intelligence efforts in Afghanistan, a reporter for the *New York Times*, "an American of Norwegian rather than Afghan extraction," voluntarily submitted to biometric database screening with the U.S. military's Biometric Automated Toolset (B.A.T.) system.[216] "After his fingerprints and iris scans were entered into the B.A.T.'s armored laptop, an unexpected 'hit' popped up on the screen, along with the photograph of a heavily bearded Afghan."[217] The biometric screening revealed the accuracy vulnerabilities that resulted in a false determination. "The 'hit' identified the reporter as 'Haji Daro Shar Mohammed,' who is on terrorist Watch List 4, with this note: 'Deny Access, Do Not Hire, Subject Poses a Threat.'"[218]

In optimal testing conditions, biometric data matching yields relatively accurate results. On a mass scale of hundreds of millions, however, a false yield rate of even one to five percent could result in the wrongful targeting of hundreds of thousands of individuals. On a mass scale of billions, a false yield rate of one to five percent could result in the wrongful targeting of millions of individuals. Nonetheless, such is the allure of biometrics and biometric intelligence that it is being actively employed to serve population management overseas and identity management domestically.

B. Population Management and Identity Management: Biometrics and Contextual Information

Biometric-enabled intelligence gathered and used domestically typically serves the purpose of "identity management," a policy term of art that supports the sorting of individuals for various security-related purposes. However, in the context of the military, the term of art is "population management." Both terms of art—"identity management" and "population management"—provide critically important policy rationales that explain, in part, the driving force that

214 *See, e.g.*, BIOMETRIC RECOGNITION, *supra* note 14, at 4–5.
215 VACCA, *supra* note 14, at 45.
216 Nordland, *supra* note 42.
217 *Id.*
218 *Id.*

may underlie the push to expand the mass collection of biometric data of entire populations and subpopulations.

The term "population management" appears to be used by the U.S. military to explain and justify the collection of the biometrics and "contextual data" of "every living person in Afghanistan."[219] The 2011 U.S. Army Commander's Guide to Biometrics in Afghanistan has a section entitled "Population Management."[220] The Commander's Guide reportedly outlines the goals of the military's population management program:

> The Commander's Guide to Biometrics in Afghanistan . . . encourages documenting as many Afghans as possible. "Every person who lives within an operational area should be identified and fully biometrically enrolled with facial photos, iris scans, and all 10 fingerprints (if present)," the guide says. (That was apparently a reference to Afghanistan's many amputees.)[221]

The 2011 U.S. Army Commander's Guide to Biometrics in Afghanistan and other documents set forth the biometric data policy in Afghanistan: "[t]he stated goal of the Afghan [biometric data collection] effort is no less than the collection of biometric data for every living person in Afghanistan."[222] To demonstrate the military resources invested in executing this objective, it was reported that in one year, from November 2010 to November 2011, "12,000 [U.S.] soldiers [in Afghanistan] have been trained to use the B.A.T."[223]

Biometric data collection has been an essential aspect of the U.S. military's ground operations in Afghanistan. "The biometric enrollment program in Afghanistan began in earnest in 2006. Since then, hundreds of thousands of biometric records have been ingested in both coalition and Afghan databases."[224] Yet, at the same time, the U.S. military has been unable to develop comprehensive, multi-modal biometric databases (e.g., comprehensive combination of digital photographs, fingerprints, iris scans, DNA, etc.) of "every living person in Afghanistan" through militarized operations and intelligence-gathering operations alone.[225] "We can't go door to door [to collect biometric

---

219 *Identity Dominance*, *supra* note 144.
220 *Id.*
221 Nordland, *supra* note 42.
222 *Identity Dominance*, *supra* note 144.
223 Nordland, *supra* note 42.
224 Pendall & Sieg, *supra* note 25, at 69.
225 *See* Nordland, *supra* note 42.

data]," explained one U.S. military leader in Afghanistan.[226] As a result, according to one media report, "the military has not conducted wholesale sweeps of communities [in Afghanistan] to gather biometrics."[227]

It is not simply the collection of Afghani biometric data, however, that accomplishes the goals of population management. "The soldiers must also record 'good contextual data' about the individual such as 'where they live, what they do, and to which tribe or clan they belong.'"[228] In other words, as discussed in Part A, raw biometric data must be fused with extensive contextual data. Population management objectives include the collection, storage, and analysis of biometric data, biographic data, and behavioral data combined:

> A checklist included in the ['Population Management'] section [of the 2011 U.S. Army Commander's Guide to Biometrics in Afghanistan] includes the following instructions:
> - Locate and identify every resident (visit and record every house and business). At a minimum, fully biometrically enroll all military-age males as follows:
>   - Full sets of fingerprints.
>   - Full face photo.
>   - Iris scans.
>   - Names and all variants of names.
>   - BAT associative elements:
>   - Address.
>   - Occupation.
>   - Tribal name.
>   - Military grid reference of enrollment.
> - Create an enrollment event for future data mining.
> - Listen to and understand residents' problems.
> - Put residents in a common database.
> - Collect and assess civil-military operations data.
> - Identify local leaders and use them to identify the populace.
> - Use badging to identify local leaders, and key personnel.
> - Cultivate human intelligence sources.
> - Push indigenous forces into the lead at every possible opportunity.
> - Track persons of interest; unusual travel patterns may indicate unusual activities.[229]

---

226 *Id.*
227 *Id.*
228 *Identity Dominance*, *supra* note 144.
229 *Id.*

The U.S. military has specifically created a "Biometrics Identity Management Agency," later renamed the Defense Forensics and Biometrics Agency, within the U.S. Department of Defense to assist in the implementation of population management goals.[230]

In the non-military context, the U.S. civilian government has structured identity management tools and programs that parallel the military's population management tools and programs in ambition. Identity management tools deployed domestically, like the population management tools currently deployed abroad militarily, represent the fusion of biometric data, biographic data, and other contextual data as a method to inform homeland security decisionmaking.

For instance, DHS offers this definition of "identity management":

> Identity Management (IdM) is a broad administrative area that deals with identifying and managing individuals within a government, state, local, public, or private sector network or enterprise. In addition, authentication and authorization to access resources such as facilities or, sensitive data within that system are managed by associating user rights, entitlements, and privileges with the established identity.[231]

As a policy prescription for a broad swath of homeland security objectives, identity management is presented as a broad umbrella that may encompass multiple goals:

> Identity management plays a critical role in a number of applications. Examples of such applications include regulating international border crossings, restricting physical access to important facilities like nuclear plants or airports, controlling logical access to shared [computerized and digitalized] resources and information, performing remote financial transactions, or distributing social welfare benefits.[232]

Biometric experts have observed that multiple post-9/11 identity management programs have mandated the use of biometrics:

> For example, the Enhanced Border Security and Visa Entry Reform Act of 2002 . . . mandated the use of biometrics in the issue of U.S.

---

230 DEF. FORENSICS & BIOMETRICS AGENCY, http://www.dfba.mil (last updated June 11, 2015).

231 *Identity Management and Data Privacy Technologies Project*, CYBER SEC. RESEARCH & DEV. CTR. (on file with author). For an overview of identity management as a policy concept, see Lucy L. Thomson, *Critical Issues in Identity Management—Challenges for Homeland Security*, 47 JURIMETRICS J. 335 (2007).

232 *See* JAIN, ROSS & NANDAKUMAR, *supra* note 14, at 1; *see also* IDMANAGEMENT.GOV, http://www.idmanagement.gov (last visited Nov. 14, 2015).

> visas. . . . [T]he US-VISIT program (United States Visitor and Immigration Status Indicator Technology) . . . validates the travel documents of foreign visitors to the United States based on fingerprints. The International Civil Aviation Organization (ICAO) has unanimously recommended that its member States use Machine Readable Travel Documents (MRTDs) that incorporate at least the face biometric (some combination of face, fingerprint and iris can also be used) for purposes of verifying the identity of the passport holder.[233]

Multiple experts have suggested that biometrics are the key to national security and homeland security in that biometric data can implement more accurate identity management systems on a mass scale, allowing the identity screening of millions and potentially billions of individuals.[234]

One option that many nations have adopted or considered adopting is a biometric-based identification card. For example, the adoption of a biometric-based "national identity card" has been considered by the Afghanistan government.[235] The efficacy of this would be to enable the U.S. military to encourage the Afghanistan government to conduct "biometric screening of the entire population" of Afghanistan through "the national identity card."[236] The "wholesale sweeps of communities to gather biometrics"[237] can thus be implemented through civilian government structures without military or intelligence intervention. Yet, at the same time, the ability of the U.S. military and intelligence community to access such biometric data, if such access is allowed, puts such data at the service of identity intelligence, biometric-enabled intelligence, and biometric cyberintelligence objectives.

An example of the military's promotion abroad of foreign governments compiling biometric data on their own citizens can be found in a January 2014 study published in National Defense University's *Joint Force Quarterly*. The study concludes that security forces in Afghanistan should "[t]reat every event as a means to collect additional biometrics."[238] Specifically, the study finds that the Afghan National Security Court has obtained convictions in "almost every case where a biometric match has been made between the defendant and the

---

233 *Id.*

234 *See id.* at 1–2.

235 Rod Nordland, *Afghanistan Has Big Plans for Biometric Data*, N.Y. TIMES (Nov. 19, 2011), http://www.nytimes.com/2011/11/20/world/asia/in-afghanistan-big-plans-to-gather-biometric-data.html?pagewanted=all&_r=0.

236 *Id.*

237 *Id.*

238 Pendall & Sieg, *supra* note 25, at 74.

criminal instrument."[239] To be clear, the U.S. military is not alone in promoting the adoption of a national biometric identity card, so its motives are likely well-intentioned. Already, as previously discussed, bureaucratized cybersurveillance systems increasingly incentivize the development of universal biometric databases of an entire citizenry, often through biometric-based national ID systems.[240] The Snowden disclosures have revealed that the NSA and foreign intelligence community appear to rely upon biometric-based national ID systems for biometric data harvesting purposes.[241]

Table 1 illustrates that there has been a growing movement internationally, particularly in the past decade, to implement digitalized biometric-based national ID systems. In the United States, this movement is often tied to comprehensive immigration reform proposals.[242] Such systems allow for biometric data to be stored, screened, and analyzed across a spectrum of agencies for multiple purposes, including identity management systems that may include identity verification and determination programs, and identity inference programs.[243]

Table 1. Nations Adopting Digitalized Biometric ID Systems

Country	Program
Albania	All Albanian citizens who are over 15 years of age must have a biometric identity card that contains fingerprints, general biographic information, and a digital photograph.[244]
Belgium	Mandatory ID cards for those over the age of 12, which contains a chip that

239 *Id.* at 72.

240 Hu, *Biometric ID*, *supra* note 28, at 1543–44.

241 *See, e.g.*, Risen & Poitras, *supra* note 31.

242 Hu, *Biometric ID*, *supra* note 28, at 1509–12.

243 *Id.* at 1508 tbl.5.

244 *Albania: The Biometric Identity Card; Its Appearance, Use and the Biometric Data Stored on It; Requirements and Procedures to Obtain a Biometric Identity Card Within Albania; Whether It Can Be Replaced and Renewed from Abroad, Including Requirements and Procedures*, REFWORLD (Sept. 22, 2011), http://www.unhcr.org/refworld/docid/4f5f1e0b2.html.

	stores the photograph as biometric data.[245]
Bulgaria	Personal ID cards contain biometric data, including fingerprints.[246]
Gabon	Currently building a national biometric civil registry, which will be the primary registry for all forms of citizen identification, including national ID cards.[247]
India	The distribution of biometric resident ID cards, which contain a photograph, biometrics, and a 64 kb smart chip, is underway.[248]
Indonesia	Electronic national ID card captures fingerprints, a photograph, and an iris scan; 118 million records are already stored in Indonesia's databases.[249]

[245] STATEWATCH, ID CARDS IN THE EU: CURRENT STATE OF PLAY (2010), http://www.statewatch.org/analyses/no-107-national-ID-cards-questionnaire.pdf.

[246] *First Domestic ID Cards Issued in Bulgaria on Monday*, NOVINITE.COM (Mar. 28, 2010, 6:46 PM), http://www.novinite.com/view_news.php?id=114680.

[247] Jill Jaracz, *Gabon Selects Gemalto for Biometric National Registry*, SECUREIDNEWS (Sept. 21, 2012), http://www.secureidnews.com/news-item/gabon-selects-gemalto-for-biometric-national-registry/?tag=biometrics&tag=Government_ID.

[248] ET Bureau, *Clash with Aadhar Cards Seen: Home Ministry's I-Card Plan Too Lands in Trouble*, ECON. TIMES (Feb. 2, 2013, 3:19 AM), http://articles.economictimes.indiatimes.com/2013-02-02/news/36703931_1_aadhaar-cards-id-cards-unique-identification-authority. Indian officials from the department of Food and Civil Supplies recently discovered that the deputy director of the department conspired with the biometric franchisee to create 150 fraudulent biometric ration cards. *Bogus Ration Cards Created with Biometrics*, DECCAN HERALD (Jan. 9, 2013), http://www.deccanherald.com/content/304160/bogus-ration-cards-created-biometrics.html; *see also* Rebecca Bowe, *India's Gargantuan Biometric Database Raises Big Questions*, ELEC. FRONTIER FOUND. (Sept. 27, 2012), https://www.eff.org/deeplinks/2012/09/indias-gargantuan-biometric-database-raises-big-questions (explaining that as of September 2012, India's Unique Identity (UID) program "ha[d] amassed a database of 200 million Indian residents' digital fingerprints, iris scans, facial photographs, names, addresses, and birthdates," with a view to capturing this information for all 1.2 billion residents).

[249] Andrew Hudson, *Indonesia Close to Rolling Out Biometric-Based National IDCard Project*, SECUREIDNEWS (Sept. 24, 2012), http://www.secureidnews.com/news-item/indonesia-close-to-rolling-out-ambitious-biometric-based-national-id-card-project/?tag=biometrics&tag=National_ID. The Indonesian government plans to use the e-KTP card for a variety of purposes such as "voter registration, passport issuance,

Italy	ID card contains a 32 kb contact chip and stores photograph and fingerprints.[250]
Lithuania	Electronic ID card contains facial image and two fingerprints.[251]
Malaysia	"[N]ational ID that uses biometric fingerprint recognition, smart card chips, and photo[graph]s."[252]
Mexico	The Personal Identity Card for minors (ages 4 to 17) is embedded with records of iris images, fingerprints, and a photograph. As of May 2012, 4 million minors were enrolled in the program. The Mexican government is extending the ID cards to adults.[253]
Mongolia	New eID program requires that all citizens over 18 years old carry smart cards as their national ID. The card contains a microprocessor that manages personal data, including a digital photograph and fingerprints.[254]

tax and financial applications." *Id.*; *see also* Ellen Messmer, *Indonesia Advances World's Most Ambitious Biometric-Based National Identity Card Project*, NETWORKWORLD (Sept. 20, 2012), http://news.idg.no/cw/art.cfm?id=EE35F375-9C4F-08CE-E838D226571E442C.

250 STATEWATCH, *supra* note 245.

251 *Id.*

252 *Biometric Uses*, ALPHACARD, http://www.alphacard.com/id-cards/biometric-uses (last visited Nov. 14, 2015).

253 Rebecca Bowe, *2012 in Review: Biometric ID Systems Grew Internationally. . . And So Did Concerns About Privacy*, ELEC. FRONTIER FOUND. (Dec. 29, 2012), https://www.eff.org/deeplinks/2012/12/biometric-id-systems-grew-internationally-2012-and-so-did-concerns-about-privacy; *see also* Gabriela Manuli, *Despite Privacy Concerns, Mexico Continues Scanning Youth Irises for ID Cards*, ELEC. FRONTIER FOUND. (Aug. 31, 2012), https://www.eff.org/deeplinks/2012/08/despite-privacy-concerns-mexico-continues-scanning-youth-irises-id-cards.

254 Zack Martin, *Mongolia Taps Gemalto for National IDs*, SECUREIDNEWS (Nov. 30, 2012), http://www.secureidnews.com/news-item/mongolia-taps-gemalto-for-national-ids/?tag=government.

Nepal	Nepal is launching the first phase of a smart card national identification program that will begin by giving 117,000 citizens smart cards embedded with personal data and a unique national ID number. The plan is to completely phase in the cards over the next 5 years.[255]
Netherlands	"[A]utomated border crossing system with photo, biometric iris recognition, and a smart card chip."[256]
Nigeria (National Identity Management Commission)	National ID card and database uses biometrics, including photograph and fingerprints, and unique numbers for every individual.[257]
Pakistan	Multi-biometric national identity card, which includes a photograph and thumbprint, has been issued to 96% of the adult population.[258]
Portugal	Mandatory "Citizen Card."[259]
Senegal	National ID card containing biometric data (fingerprints and photograph) is

[255] *Govt to Distribute 117,000 Biometric IDs in Next 18 Months*, MYREPÚBLICA (Aug. 17, 2016, 2:00 AM), http://www.myrepublica.com/news/3966.

[256] *Biometric Uses*, *supra* note 252.

[257] *Nigeria: The Issuance of National Identity Cards After 2003; Description of the Card; Prevalence of False National ID Cards; Introduction of the New Card (2003–July 2008)*, REFWORLD (Aug. 5, 2008), http://www.unhcr.org/refworld/docid/48d2237734.html.

[258] *Pakistan: Computerized National Identity Cards (CNICs), Including Overseas Identity Cards; Issuance Procedures*, REFWORLD (Jan. 7, 2013), http://www.unhcr.org/refworld/docid/510f9cef2.html. The Computerized National Identity Card (CNIC) is required for various activities, including obtaining a passport or driver's license, holding a job, registering to vote, using social services, and opening a bank account. *Id.*

[259] *Portuguese Citizen ID Card Roll Out Underway*, BIOMETRIC TECH. TODAY, Feb. 2007, at 3.

	mandatory for everyone 15 years of age or older.[260]
Republic of Serbia	Each citizen over the age of 16 must carry an identity card containing biographic and biometric data, including a photograph and fingerprint.[261]
Spain	"[S]ocial Security card with biometrics and a smart card chip for storing information."[262]
Sweden	ID card contains a radiofrequency (RFID) chip for biometric data.[263]

C. Identity Dominance and Big Data Cyberintelligence

Like population management, "identity dominance" appears to be another term of art in the military and intelligence community. However, it has no domestic counterpart like identity management. This is not surprising given that identity dominance evokes an adverse relation to the population subject to the data collection and subsequent dominance. Specifically, it appears that identity dominance expresses a strategic military and intelligence goal of digital data dominance in the realm of biometric data and contextual information. Gregory Sieminski, Chief of the Identity Intelligence Division, National Ground Intelligence Center, U.S. Army, explained, "BEI has saved countless lives in Iraq and Afghanistan and helped our forces achieve identity dominance in demanding insurgency environments."[264] According to one media report, the U.S. military's goal of identity dominance can be explained and rationalized this way: "By collecting vast amounts of information on the population of Afghanistan, . . . the U.S. military has sought to achieve *identity dominance* by

---

260 *Senegal: The Procedures for Obtaining a Birth Bulletin and a National Identity Card*, REFWORLD (Feb. 27, 2007), http://www.unhcr.org/refworld/docid/469cd6997.html; *see also* Mariama Mary Fall Dia, *UNHCR Distributes Biometric ID Cards to Refugees in Senegal*, UN REFUGEE AGENCY (Oct. 22, 2012), http://www.unhcr.org/508536389.html.

261 MINISTRY OF INTERIOR, REPUBLIC OF SERB., OFFICIAL GAZETTE OF THE REPUBLIC OF SERBIA, NO. 62/06, IDENTITY CARD LAW (2008).

262 *Biometric Uses*, *supra* note 252.

263 STATEWATCH, *supra* note 245.

264 Moruza, *supra* note 26.

undermining the fluid anonymity of terrorist and criminal networks and attaching permanent [biometrically-enabled] identities to malicious actors."[265]

Nevertheless, the U.S. Army, for instance, has pointed out the benefits of biometric-based identity dominance in Afghanistan that tracks the purported domestic homeland security advantages that appear to animate DHS's expansion of biometric data collection within the United States through identity management rationales:

> [T]he commander of the U.S. Army's Task Force Biometrics Col. Craig Osborne [explained] that the collection of biometric data is not simply about "identifying terrorists and criminals," but that "it can be used to enable progress in society and has countless applications for the provision of services to the citizens of Afghanistan." According to Osborne, biometrics provide the Afghan government with "identity dominance" enabling them to know who their citizens are and link actions with actors.[266]

To further demonstrate the perceived holistic value of biometric data to the military, it is useful to refer to the U.S. Department of Defense's instructional guidelines on biometric-enabled intelligence, titled "Defense Biometric Enabled Intelligence (BEI) and Forensic Enabled Intelligence (FEI)."[267] The instructional guidelines explain that "[i]n addition to the traditional intelligence cycle functions, BEI and FEI shall: (1) Collect, digitize, and transmit biometric data at the tactical, operational, and strategic levels."[268] Therefore, identity dominance—as executed through biometric data collection and analysis—is purported to advance multiple benefits at all levels of military decisionmaking: tactical, operational, and strategic.

Specifically, "[o]ver the last decade, biometrics has been put to use for improvised explosive device forensics and for identifying and targeting suspected insurgents and terrorists."[269] According to official U.S. government reports and representations, biometric-enabled intelligence allows for the military to make more informed operational and tactical decisionmaking in the following ways:

---

265 *Identity Dominance*, *supra* note 144.

266 *Id.*

267 U.S. DEP'T OF DEF., *supra* note 155. Preceding this document, the media outlet states: "The following instruction is part of a series of 'limited release' DoD doctrine publications that are not released to the public." *(U//FOUO) DoD Instruction: Biometric Enabled Intelligence (BEI) and Forensic Enabled Intelligence (FEI)*, PUB. INTELLIGENCE (Aug. 10, 2013), http://publicintelligence.net/dod-biometric-intelligence/.

268 U.S. DEP'T OF DEF., *supra* note 155, at 2.

269 Iannotta, *supra* note 24.

> Incident tracking and analysis will discern patterns and enable better planning for security operations. Units should never enter an area for targeting raids, deliberate detentions, or clearance operations without knowing who they will likely encounter. . . . The BEI-based process of developing biometric named areas of interest allows units at all levels to pull the known entities from the database and plot them (by site of enrollment or by associated event location) on the operations graphic as an overlay. Units can review the density of previously enrolled individuals, review in aggregate or by individual, assess threats based on matches to security incidents, and better predict where these individuals are likely to be ahead of the operation, especially when they integrate the biometrics with other all-source intelligence as part of the intelligence preparation.[270]

Consequently, the U.S. military explains that biometrics is an essential tool for the warfighter.[271] "U.S. military officials say biometrics have become a useful battlefield tool in Iraq and Afghanistan . . . ."[272] Since 2010, the Defense Forensics and Biometrics Agency (DFBA) has been in the process of being converted from a temporary task force to a permanent component of the U.S. Department of Defense.[273] DFBA (then BIMA) explains: "This transformation reflects both the successes biometrics have had in supporting the warfighter and protecting our country and allies from terrorism and the vision of what biometrics can bring to the DoD in the future."[274] This has led at least one military official, Air Force General Victor Renuart, to announce that more biometric data collection is needed domestically, apparently, in part, to assist the military in its war effort abroad: "'Interestingly, we are probably further forward in using biometrics outside our country in some of the combat environments than we are inside our country,' said the general. 'We've got to find a way to fix that.'"[275]

Biometric-enabled intelligence is gaining widespread acceptance as an essential battlefield tool by the U.S. military. But the fields of biometric-enabled

---

[270] Pendall & Sieg, *supra* note 25, at 74 (emphasis omitted).

[271] BIOMETRICS TASK FORCE, U.S. DEP'T OF DEF., ANNUAL REPORT FY 2009, Director's Message at 1, https://fas.org/man/eprint/biometric09.pdf.

[272] *Biometric System Working in Afghanistan*, UNITED PRESS INT'L (July 14, 2011, 10:03 AM), http://www.upi.com/Top_News/US/2011/07/14/Biometric-system-working-in-Afghanistan/UPI-74141310652220/.

[273] BIOMETRICS TASK FORCE, *supra* note 271, Director's Message at 1. As noted above, BIMA was renamed the Defense Forensics and Biometric Agency in 2013. *See supra* note 230 and accompanying text.

[274] *Id.*

[275] Nathan Hodge, *General Wants to Scan More U.S. Irises, Fingerprints*, WIRED (Jan. 29, 2009, 2:00 PM) http://www.wired.com/dangerroom/2009/01/biometrics-need/.

intelligence and biometric cyber intelligence are still emerging in the traditional intelligence community.[276] "Biometrics has evolved dramatically during the Iraq and Afghanistan conflicts, . . . but the discipline has not been fully institutionalized into the intelligence community."[277] One military specialist explained that "[a]s BEI tradecraft is spread beyond its current wartime origins, more and more Army intelligence analysts are learning the power of fusing biometrics data with other, more traditional sources of intelligence."[278] "The intelligence community is pushing to make biometrically enabled intelligence—the art of identifying people by fingerprints, digital mugshots, iris scans or DNA—a regular part of business."[279]

D. Interoperable Biometric Databases and the Bureaucracy of Biometric Data Management

To achieve the goals of identity management and population management, the cybersurveillance strategy must be comprehensive in scope. Therefore, the data must be shared and exploited across multiple domains. For example, when the U.S. military collects biometric data for one purpose, it is shared with other databases. "Gathering the data does not stop at Afghanistan's borders, . . . since the military shares all of the biometrics it collects with the United States Department of Justice and the Department of Homeland Security through interconnected databases."[280] Once the data is captured and analyzed, it is difficult to protect against potential data breaches and data compromises, as well as potential data abuses and data privacy violations.[281] Other issues include interoperability between platforms, data quality at the time of biometric capture, and other variables that may ultimately impact the integrity of the data screening or data analysis.

Table 2 shows that within the U.S. and internationally, multiple agencies and bureaucracies have emerged in the past decade to manage the flow of biometric data: the capture, storage, and analysis of biometrics for identity management and population management goals. Increasingly, these goals integrate the objectives of the military and intelligence community.

---

276 Iannotta, *supra* note 24.

277 *Id.*

278 Moruza, *supra* note 26 (quoting Specialist Kama Mountz, 500th Military Intelligence Brigade).

279 Iannotta, *supra* note 24.

280 Nordland, *supra* note 42.

281 BENJAMIN WITTES, BROOKINGS INST. DATABUSE: DIGITAL PRIVACY AND THE MOSAIC 18 (2011), https://www.brookings.edu/research/databuse-digital-privacy-and-the-mosaic/.

Table 2. Examples of Bureaucracies Managing and Sharing Biometric Data

Program	Agency	Purpose
Defense Forensics & Biometrics Agency (DFBA) (formerly the Biometrics Identity Management Agency (BIMA))[282]	DoD/U.S. Army	Permanent agency that "represents the synthesis of Department of Defense (DoD) capabilities in forensics and biometrics."[283] Also in charge of the DoD Biometric Enterprise Strategic Plan.[284]
Biometric Center of Excellence (BCOE)	FBI	Created in 2007 to support the FBI's overall biometric mission by advancing the use of new biometric technologies.[285]
Biometric Standards Program and Resource Center	National Institute of Standards and Technology (NIST)	To assist both the U.S. government and private sector by "[s]upporting the national strategy on biometrics."[286]
Biometrics Subcommittee of the National Science	The White House (Office of Science and Technology Policy)	"[S]hapes national efforts and coordinates with Federal agencies that

[282] *DFBA FAQs*, DEF. FORENSICS & BIOMETRICS AGENCY, http://www.dfba.mil/About/faqs.aspx (last visited Nov. 14, 2016).

[283] *Id.*

[284] According to the DoD, "[t]he DoD Biometrics Enterprise will change focus from primarily being a 'Wartime' need to 'Peacetime' activities." BIOMETRICS IDENTITY MGMT. AGENCY, DOD BIOMETRICS COLLABORATION FORUM 9 (2011), http://www.dtic.mil/dtic/tr/fulltext/u2/a550048.pdf.

[285] *About the Biometric Center of Excellence*, FBI, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/biometric-center-of-excellence/about-the-biometric-center-of-excellence (last visited Nov. 14, 2016).

[286] *Biometric Standards Program and Resource Center*, NAT'L INST. STANDARDS & TECH., http://www.nist.gov/itl/csd/scm/biometric-standards.cfm (last updated Sept. 21, 2016).

and Technology Counsel (NSTC)		have an interest in biometrics. . . . [And] dedicated to finding the best ways to achieve realtime identification and tracking and to increase personal, corporate, and government security."[287]
Information Awareness Office (IAO)	Defense Advanced Research Projects Agency (DARPA)	Created in 2002 to "integrate advanced technologies and accelerate their transition to operational users."[288]
DoD Identity Protection and Management Senior Coordinating Group (IPMSCG)	DoD	Provides strategic guidance to the Common Access Card (CAC) program, the Public Key Infrastructure (PKI) program, and the DoD Biometrics program.[289]
DHS Biometrics Coordination Group	DHS	"[F]ocal point for intra-departmental planning and coordination on biometrics RDT&E [research, development, testing, and evaluation] and deployment to operational end-users."[290]

[287] *Biometrics*, NAT'L INST. JUSTICE, http://www.nij.gov/topics/technology/biometrics/welcome.aspx (last updated Sept. 15, 2011).

[288] REPORT TO CONGRESS REGARDING THE TERRORISM INFORMATION AWARENESS PROGRAM 1 (2003) http://epic.org/privacy/profiling/tia/may03_report.pdf.

[289] U.S. DEP'T OF DEF., INSTRUCTION NO. 1000.25, DOD PERSONNEL IDENTITY PROTECTION (PIP) PROGRAM (2016), http://www.cac.mil/docs/DoDI-1000.25.pdf.

[290] NAT'L SCI. & TECH. COUNCIL, BIOMETRICS IN GOVERNMENT POST-9/11 (2008), http://www.biometrics.gov/Documents/Biometrics%20in%20Government%20Post%209-11.pdf.

Office of Consular Systems and Technology (CST)	DoS	Manages biometrics for Department of State programs such as the Consular Consolidated Database (CCD) and the Border Crossing Card project.[291]
Biometrics Section of the National Institute of Justice (NIJ)	DOJ	Participates in the Biometrics Subcommittee of the National Science and Technology Council; some of the NIJ's research priorities are confirming the identity of individuals, identifying individuals based on surveillance, and the collection of biometrics in field environments.[292]
Biometrics Institute	Independent organization (over 190 members worldwide from public sector, private sector, and academia)[293]	"[T]o promote the responsible use of biometrics as an independent and impartial international forum for biometric users and other interested parties."[294]

[291] Alex Olesker, *Department of State's Consular Systems and Technology: A Track Record of Innovation*, CTOVISION.COM (Oct. 7, 2011), http://ctovision.com/2011/10/department-of-states-consular-systems-and-technology-a-track-record-of-innovation/.

[292] *Biometrics*, *supra* note 287.

[293] *List of Members*, BIOMETRICS INST., http://www.biometricsinstitute.org/pages/list-of-members.html (last visited Nov. 14, 2016).

[294] *Mission*, BIOMETRICS INST., http://www.biometricsinstitute.org/pages/mission.html (last visited Nov. 14, 2016).

Aviation Security Biometrics Working Group (ASBWG)	FAA/DoD	Working group created in 2001 to analyze the efficacy of implementing biometrics into airport security systems.[295]
DoD Biometrics Executive Committee (EXCOM)	DoD	Focal point for coordination of biometric programs; voting members include general officers from the U.S. Army, Navy, Marine Corps, and Air Force.[296]
Joint Biometrics Operational Coordination Board (JBOCB)	DoD	Tasked with gathering operational requirements and resolving issues that affect the "joint biometrics enterprise."[297] It includes all DoD Biometrics stakeholders such as Combatant Commands, agencies, Joint Staff, and Office of the Secretary of Defense.[298]

III. THE RELATIONSHIP BETWEEN BIOMETRIC CYBERSURVEILLANCE AND BIOMETRIC CYBERINTELLIGENCE

The role biometric-enabled intelligence has played in U.S. operations in Afghanistan illustrates the breadth of military- and intelligence-related purposes served by biometrics as the U.S. military has "developed an extensive repository

295 NAT'L SCI. & TECH. COUNCIL, *supra* note 290.

296 U.S. DEP'T OF DEF., DIRECTIVE NO. 8521.01E, DOD BIOMETRICS (2016), http://www.cac.mil/docs/8521.01-DoD-Biometrics.pdf.

297 BIOMETRICS TASK FORCE, ANNUAL REPORT FY07 (2007), https://www.hsdl.org/?view&did=27030.

298 *Id.*

of biometric data across Afghanistan."[299] In particular, according to the U.S. military:

> [M]odes of biometric data allow both coalition and Afghan forces to protect themselves by ensuring that the ANSF [Afghan National Security Forces], local national workforce, Afghan Local Police, and reintegrating insurgents (and criminals) are who they say they are and can be screened against derogatory information (matches for previous incidents such as improvised explosive device [IED] attacks and other events that leave biometric information behind).[300]

A database to enable nationwide identification and screening demonstrates the ways in which biometric data collected by the military and intelligence community may lead to long-term cybersurveillance consequences. As biometric databases may be increasingly shared between military, intelligence, and law enforcement organizations and other public and private entities, the biometric database screening systems may be increasingly integrated with other behavioral and contextual databases (e.g., consumer patterns, web browsing activity, data brokers predicting sexual orientation and religion, etc.) and biographical databases (e.g., passport databases, driver's license databases, etc.).

In this Part, the discussion first explores how surveillance technology designed for military and foreign intelligence purposes may migrate to domestic law enforcement uses. Part III.A looks briefly, but specifically, at digital watchlisting programs which tend to be anchored with biometric data. Part III.B focuses on military targeting based on cybersurveillance and biometrics. This technology does not appear to have migrated to domestic law enforcement use, it is relevant to any effort to interrogate the expanding capacities of biometric enabled intelligence.

A. Biometrics in Intelligence-Driven Decisionmaking and Biometric-Based Digital Watchlisting

One method of biometric surveillance that has been accepted by the intelligence community and is being used concurrently for military purposes abroad, as well as domestically, is digital watchlisting. "As with the military's biometric data, information on each person is fed into a computer to find those

---

299 Pendall & Sieg, *supra* note 25, at 69.
300 *Id.* at 70.

who are on terrorist watch lists, have outstanding criminal warrants or even are just businessmen under investigation."[301]

Since the terrorist attacks of September 11, 2001, the U.S. domestic and foreign intelligence community and homeland security structure has developed extensive database screening systems and watchlisting programs, including the "No Fly List," the "Terrorist Watchlist," the "Disposition Matrix," and the "Kill List."[302] Abroad, the U.S. military has developed "Be on the Lookout" (BOLO) lists and database screening systems, and other watchlists.[303] Increasingly, in Afghanistan, these database screening systems and watchlisting programs rely upon biometric data as a data backbone for screening purposes.[304]

> [A]ccording to Col. Fred Washington, director of the United States Army's biometrics task force[:] Since 2007, when biometric collection began in Afghanistan, biometrics have been used to identify 3,000 suspects on either Watch List 1 or Watch List 2, the American military's two most serious classifications for possible insurgents or terrorists. In many cases, fingerprints found on bomb remains have identified the bomb maker . . . .[305]

> Across Regional Command–East (RC-E) [Afghanistan], biometric intelligence-driven operations have achieved major impacts on the insurgent ability to maintain leadership and lower-level cell structures as both coalition and Afghan forces regularly employ biometrically developed insurgent watch lists and 'be on the lookout' (BOLO) messages and as they execute deliberate detention operations.[306]

Digital watchlists seem like the most natural and basic outgrowth of compiling biometric databases with nationwide aspirations, so their appearance both domestically and in combat zones is no surprise. At the most basic level, contextual data enables authorities to identify suspects fitting certain profiles, and biometric data allows the biographical profile to be pinned to a living human body.

---

301 Nordland, *supra* note 42.

302 Ian Cobain, *Obama's Secret Kill List—The Disposition Matrix*, THE GUARDIAN (July 14, 2013, 2:00 PM), https://www.theguardian.com/world/2013/jul/14/obama-secret-kill-list-disposition-matrix. *See also* Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735, 1773–76, 1786–92 (2015) (discussing background and due process risks of No Fly List and Terrorist Watchlist).

303 Pendall & Sieg, *supra* note 25, at 69.

304 Nordland, *supra* note 42.

305 *Id.*

306 Pendall & Sieg, *supra* note 25, at 69.

B. Biometric Cyberintelligence and NSA Cybersurveillance

Due to the covert nature of drone attacks, limited information is available on the exact nature of NSA cybersurveillance, including biometrically-enabled intelligence that may inform targeted killings.[307] Recent Snowden disclosures have revealed, however, that the NSA collects millions of digital photographs from Internet and social media sources and utilizes facial recognition technology to identify individuals for "precision targeting" purposes.[308] According to these disclosures, the NSA's "reliance on facial recognition technology has grown significantly over the last four years as the agency has turned to new software to exploit the flood of images included in emails, text messages, social media, videoconferences and other communications."[309]

The recent Snowden disclosures on NSA cybersurveillance programs and other media reports also appear to indicate that biometric data,[310] if and when integrated with other dataveillance and cybersurveillance systems, may inform targeted killing technologies.[311] Other media reports prior to the Snowden disclosures have indicated that the U.S. military is awarding contracts to develop the integration of biometric data into targeting technologies.[312] Emerging big data cybersurveillance systems that integrate biometric technologies are championed as effective intelligence tools necessary to identify potential

---

307 *See generally* DAVID E. SANGER, CONFRONT AND CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER 241–70 (2012) (describing use of drones and targeted killing strategy in the "war on terror").

308 Risen & Poitras, *supra* note 31.

309 *Id.*

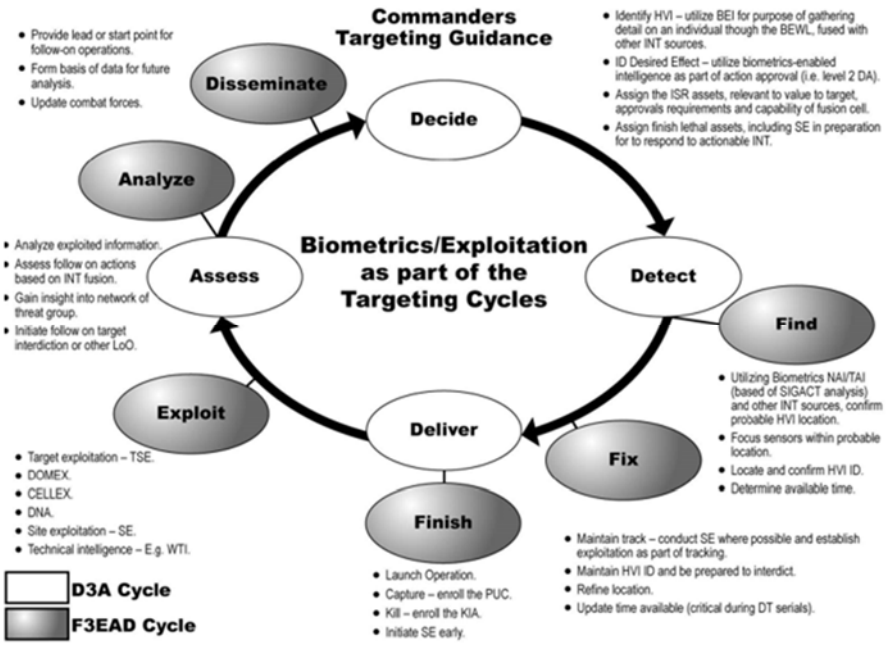
310 *See, e.g.*, *id.* (explaining that the Snowden disclosures revealed the NSA collects millions of digital photographs from Internet and social media sources and utilizes facial recognition technology to identify individuals).

311 *See, e.g.*, Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, WASH. POST (Dec. 4, 2013), https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html; Greg Miller, Julie Tate & Barton Gellman, *Documents Reveal NSA's Extensive Involvement in Targeted Killing Program*, WASH. POST (Oct. 16, 2013), https://www.washingtonpost.com/world/national-security/documents-reveal-nsas-extensive-involvement-in-targeted-killing-program/2013/10/16/29775278-3674-11e3-8a0e-4e2cf80831fc_story.html ("[A] collection of records in the Snowden trove . . . make clear that the drone campaign—often depicted as the CIA's exclusive domain—relies heavily on the NSA's ability to vacuum up enormous quantities of e-mail, phone calls and other fragments of signals intelligence, or SIGINT."); Jeremy Scahill & Glenn Greenwald, *The NSA's Secret Role in the U.S. Assassination Program*, INTERCEPT (Feb. 10, 2014, 12:03 AM), https://theintercept.com/2014/02/10/the-nsas-secret-role/ (explaining accuracy limits of what metadata-driven intelligence can yield in identifying appropriate targets for drone strikes).

312 *See, e.g.*, Noah Shachtman, *Army Tracking Plan: Drones that Never Forget a Face*, WIRED (Sept. 28, 2011, 6:30 AM), http://www.wired.com/dangerroom/2011/09/drones-never-forget-a-face.

terrorists through, for example, "integrat[ing] data from informants' tips, drone footage, and captured phone calls."[313]

Infograph 1 demonstrates the manner in which biometric data and big data's mass integrative systems help to inform cyberintelligence operations. Importantly, at the end of an operation, after "Deliver[y]," the "Finish" stage entails biometric enrollment—regardless of whether the result of delivery is a prisoner of war or an individual killed in action. Whatever role biometrics may play in targeting, the result, where possible, entails the collection of ever more biometric data.



Infograph 1. Commanders Targeting Guidance: Biometrics/Exploitation as Part of the Targeting Cycles: U.S. Army[314]

313 *Id.*

314 CTR. FOR ARMY LESSONS LEARNED, NO. 11-25, HANDBOOK: COMMANDER'S GUIDE TO BIOMETRICS IN AFGHANISTAN 29 fig.4-1 (2011), https://info.publicintelligence.net/CALL-AfghanBiometrics.pdf.

To help explain why biometric cyberintelligence holds such appeal and why and how the rapid expansion of biometric cybersurveillance strategies is a military and intelligence priority, Table 3 focuses on how digitalized biometric data is increasingly integrated into weaponry generally and biometric drone weaponry in particular.

Table 3. Biometric-Centered Weaponry and Biometric Drone Weaponry

Program	Agency	Purpose
Georgia Tech aerial drone project	Georgia Tech/DoD[315]	Aerial drones combine facial recognition technology with targeting abilities.[316]
Image Acquisition and Exploitation Camera System	ACAGI Inc., a Maryland defense technology company[317]	The facial recognition system connects to a portable database containing more than 1 million faces. The camera can be placed into the optics of a soldier's weapon, while the battery and processor are attached to the soldier's vest.[318]
Long Range, Non-Cooperative, Biometric Tagging, Tracking	Progeny Systems Corporation/U.S. Army	Company received an Army contract to develop this "drone-mounted" system

[315] *Cf.* Peter Finn, *A Future for Drones: Automated Killing*, WASH. POST (Sept. 19, 2011), https://www.washingtonpost.com/national/national-security/a-future-for-drones-automated-killing/2011/09/15/gIQAVy9mgK_story.html?utm_term=.61c151a5e71a.

[316] *Id.*

[317] Martin Barillas, *New Military Applications for Facial Recognition Technology*, SPERO NEWS (Sept. 2, 2012), http://www.speroforum.com/a/HCESHCICAJ39/73073-New-military-applications-for-facial-recognition-technology.

[318] *Id.* According to Jim Gavrilis of ACAGI, the technology "has met with a favorable reception in testing by the armed forces of the U.S. and allied countries." *Id.*

and Location System		adapted for battlefield conditions.[319]
LS3	Boston Dynamics/DARPA	Semi-autonomous drone designed to accompany ground troops, traverse difficult terrain, and carry up to 400 pounds of weaponry.[320]
"[E]ye-slaved" drone	ISCAN	A small drone, fitted with explosives, is wirelessly controlled by an eye-tracking headset. "[The drone] can be sent to blow up whatever the wearer is looking at."[321]

Other recent media disclosures have offered information on advancements in drone video and imagery technology. Gorgon Stare technology, for instance, enables the U.S. Air Force to "transmit live video images of physical movement across an entire town."[322] Gorgon Stare, made of nine video cameras mounted on a drone, is designed to send up to sixty-five different images to multiple

[319] Shachtman, *supra* note 312; *136 Phase I Selections from the 11.1 Solicitation*, ARMY, https://sbir.defensebusiness.org/content/static/selections/abs2011-1/armyabs111.html (last visited Dec. 23, 2016). According to the Army, this development in tagging, tracking, and locating (TTL) "overcomes a basic limitation in current TTL operations where inclement weather and objects of interest only appear[] periodically from sheltered positions or crowds." *Long Range, Non-Cooperative, Biometric Tagging, Tracking and Location*, SBIR SOURCE, https://sbirsource.com/sbir/topics/85875 (last visited Nov. 14, 2016).

[320] Christopher MacManus, *DARPA's Latest Footage of LS3 Robodog Astounds*, CNET (Dec. 20, 2012, 4:39 PM), https://www.cnet.com/news/darpas-latest-footage-of-ls3-robodog-astounds/; *see also The Future of Drones: Pack Mules and Camera Grenades*, BBC NEWS (Aug. 10, 2012, 4:34 AM), http://www.bbc.com/news/world-us-canada-19169023. The LS3 is not currently a biometric form of weaponry. However, given the advancement of facial recognition technology and tracking in compact systems, these technologies could be combined in the near future.

[321] *The Eyes Have It*, ECONOMIST (Dec. 1, 2012), http://www.economist.com/news/technology-quarterly/21567195-computer-interfaces-ability-determine-location-persons-gaze.

[322] Ellen Nakashima & Craig Whitlock, *With Air Force's Gorgon Drone 'We Can See Everything'*, WASH. POST (Jan. 2, 2011, 12:09 AM), http://www.washingtonpost.com/wp-dyn/content/article/2011/01/01/AR2011010102690.html.

users.[323] ARGUS-IS, another recent advancement in imagery technology, can be drone-mounted and, from 17,500 feet, can capture objects as small as six inches on the ground.[324] Further, ARGUS-IS possesses significant storage capacity, approximately one million terabytes of data per day, which can facilitate the cybersurveillance capacities of drones.[325] Recent Snowden disclosures on biometric data indicate that "[t]he [NSA] has created teams of 'identity intelligence' analysts who work to combine the facial images with other records about individuals to develop comprehensive portraits of intelligence targets. The [NSA] has developed sophisticated ways to integrate facial recognition programs with a wide range of other databases."[326] As digitalized biometric data is increasingly integrated into weaponry technologies, including biometric drone weaponry and targeting technologies, the fusion of biometric data intelligence systems with drone surveillance technology deserves close attention.

Yet, increasingly, and perhaps ironically, identity management technologies and identity dominance capacities allow the U.S. government to infer risk from suspicious digital data alone, without information on the actual identity of the target. For example, "a controversial [targeted killing] practice known as signature strikes . . . [targets those with] defining characteristics associated with terrorist activity, but whose identities aren't necessarily known."[327] Signature strikes allow the intelligence community "to hit targets based solely on intelligence indicating patterns of suspicious behavior."[328] From media reports, it appears that signature strikes are informed in part by drone footage and potentially from other types of cybersurveillance.[329] In other words, the use of signature strikes allows for drone attacks based upon suspicious data points, even when the identity of the individual targeted is unknown.

---

323 *Id.*

324 Damien Gayle, *The Incredible U.S. Military Spy Drone That's So Powerful It Can See What Type of Phone You're Carrying from 17,500Ft*, DAILY MAIL (Jan. 28, 2013, 2:56 PM), http://www.dailymail.co.uk/sciencetech/article-2269563/The-U-S-militarys-real-time-Google-Street-View-Airborne-spy-camera-track-entire-city-1-800MP.html.

325 *Id.*

326 Risen & Poitras, *supra* note 31.

327 DANIEL KLAIDMAN, KILL OR CAPTURE: THE WAR ON TERROR AND THE SOUL OF THE OBAMA PRESIDENCY 41 (2012).

328 Greg Miller, *CIA Seeks New Authority to Expand Yemen Drone Campaign*, WASH. POST (Apr. 18, 2012), http://www.washingtonpost.com/world/national-security/cia-seeks-new-authority-to-expand-yemen-drone-campaign/2012/04/18/gIQAsaumRT_story.html.

329 *See, e.g.*, *id.*

Some experts have concluded that "[t]he vast majority of drone strikes conducted by the CIA have been signature strikes."[330] The efficacy of targeting individuals for killing based on suspicious digital data requires close scrutiny. "[C]lassified government documents show[] that the drone strikes had killed hundreds of low-level suspected militants whose identities were not known."[331] Nevertheless, the future of the Disposition Matrix and Kill List may be tied more and more to biometric identification technologies and mass cybersurveillance systems.

C. The Posse Comitatus Act's Potential to Limit Militarized Cybersurveillance in Civilian Contexts

Following September 11, 2001, the U.S. military and the intelligence community have maintained an extensive presence in numerous foreign countries among populations that often contain large segments with a hostile or insurgent response to the United States' presence. Accordingly, technologies of identity management—of which biometric ID cybersurveillance is one tool—have become central to military population management. Consequently, there has been an expanded use of biometric data collection, storage, and analysis by the intelligence community and the armed services for purposes of strategic intelligence and military defense. Those biometric databases, in turn, now facilitate new forms of big data tracking and may entail unknown mass surveillance and mass targeting consequences. The integration of biometric database screening and biometric targeting into biometric drone weaponry and targeting drone strike technologies demonstrates the potential lethality of the emerging technological and policy development of biometric cyberintelligence.

Importantly, the Snowden disclosures and recent criminal law cases show how big data cybersurveillance technologies deployed by military operations and the foreign intelligence community can facilitate law enforcement and prosecutorial activities. This cooperative data-sharing, or data-commingling, environment is now made possible by big data's mass integrative potential. It necessitates careful scrutiny in that, historically, the PCA, Fourth Amendment, and other laws have been read to prohibit this cooperation to protect the separation of powers and to protect civilians from mass, indiscriminate

---

330 Kevin Jon Heller, *'One Hell of a Killing Machine': Signature Strikes and International Law*, 11 J. INT'L CRIM. JUST. 89, 90 (2013).

331 Scott Shane, *Rights Groups, in Letter to Obama, Question Legality and Secrecy of Drone Killings*, N.Y. TIMES (Apr. 12, 2013), http://www.nytimes.com/2013/04/13/us/politics/rights-groups-question-legality-of-targeted-killing.html.

surveillance activities. Significantly, though, recent criminal cases demonstrate the manner in which incriminating data—gathered either inadvertently or deliberately by intelligence activities, and at times gathered against average civilians and non-terrorist targets in mass data sweeps—can be shared with domestic law enforcement to enable prosecution. The fusion of biometric database matching systems with biographic and behavioral database matching systems, and the way in which this data fusion process can lead to policymaking, is transforming in a way that is more proactive and offensive in nature. It is presented, however, as a policymaking justification that is reactive and defensive in nature.

The recent Ninth Circuit case of *United States v. Dreyer* provides an example of the migration of cybersurveillance technologies. It illustrates how cybersurveillance technology designed for foreign intelligence and military intelligence purposes can be used to enforce civilian laws through local and state law enforcement. Confronted with the application of military cybersurveillance of a civilian populace, the Ninth Circuit rejected the claim that such sweeping surveillance is permissible so long as its overall purpose is to root out military personnel engaged in unlawful activity. It further reserved the right to suppress evidence gathered through such cybersurveillance in the future where it violates the PCA. The result of *Dreyer*—in the form of the Ninth Circuit's consideration of the possible remedy of excluding evidence and potentially overturning a criminal conviction of a person trafficking in child pornography[332]—reflects the Ninth Circuit's concern about the breadth of the cybersurveillance employed as much as a concern with the Navy's improper involvement in the enforcement of civilian laws.

This Ninth Circuit case is historic in that it is the first time that a federal court has applied the PCA, intended to ensure recognition of a proper division between military and civilian activities, as a method to warn against military intelligence data gathering for domestic cybersurveillance overreach. In *Dreyer*, the PCA served as a statutory prohibitionon governmental cybersurveillance overreach, but only because the Ninth Circuit asserted that the PCA is grounded in constitutional norms—the necessary prerequisite to making exclusion a remedy for PCA violations. The court's characterization of the PCA as constitutionally grounded may not survive Supreme Court scrutiny.

[332] United States v. Dreyer, 804 F.3d 1266, 1278–81 (9th Cir. 2015) (en banc).

The argument in favor of the Ninth Circuit's view is set out most strongly by the concurring opinion of Judge Marsha Berzon, which contends that the very structure of the Constitution reflects the importance of keeping the civilian and military spheres separate with the latter subordinate to the former.[333] However, the argument in favor of the constitutional roots of the Posse Comitatus Act is a structural one. It is dependent upon showing how various constitutional amendments and clauses restrain and restrict military prerogatives when they collide with civilian rights. This dependency, therefore, also points out the Posse Comitatus Act's vulnerability—the lack of any express constitutional language prohibiting military enforcement of civilian laws. Judge John Owens's concurrence took issue with this view, deriding the "abstract constitutional principle" the court purported to find in the Constitution and noting that if such a principle existed, the Posse Comitatus Act would not be necessary to restrain the Executive Branch from resorting to military enforcement of civilian laws, as happened in the nineteenth century.[334] Moreover, Judge Owens noted that unlike the Fourth and Fifth Amendments, which are clearly designed to protect individual rights, the PCA's protections seem oriented more generally towards the people as a whole.[335]

The constitutional question is complicated, but, in the context of cybersurveillance, increasingly important. The Constitution clearly contains provisions designed to hinder and limit a standing army,[336] just as it also provides for the military to establish order during times of emergency—for example through congressional authority to call up "the Militia to execute the Laws of the Union, suppress Insurrections and repel Invasions."[337] The PCA accounts for exceptions like the latter constitutional provision by limiting its reach only to those instances not "expressly authorized by the Constitution or Act of Congress."[338] The existence of such exceptions makes it all the more difficult to argue that the PCA expresses a constitutional norm. Yet, that is precisely what some members of Congress understood when enacting the PCA.[339]

---

333 *Id.* at 1281–83 (Berzon, J., concurring).

334 *Id.* at 1284–85 (Owens, J., concurring in the judgment).

335 *Id.* at 1285.

336 U.S. CONST. art. I, § 8 (limiting appropriations to support armies to a two-year limit).

337 *Id.*

338 18 U.S.C. § 1385 (2012).

339 *See* 7 Cong. Rec. 4240 (1878) (remarks of Sen. Kernan); 7 Cong. Rec. 4243 (1878) (remarks of Sen. Merrimon); United States v. Walden, 490 F.2d 372, 375 (4th Cir. 1974) ("several senators expressed the opinion that the Act was no more than an expression of constitutional limitations on the use of the military to enforce civil laws").

Finally, it is worth discussing a 1974 Fourth Circuit PCA case, *United States v. Walden*.[340] There, as with *Dreyer*, the court considered whether PCA-like restrictions were applicable.[341] As with *Dreyer*, the Fourth Circuit declined to suppress evidence but chose to reserve such a remedy in case future military conduct warranted it.[342] And like the *Dreyer* panel decision, the Fourth Circuit did not assess whether the PCA was grounded in the Constitution, but it did query whether PCA-like violations also presented constitutional violations.[343] However, the court's examination of the issue was inconclusive because the Navy's PCA-like restrictions provided a standard to evaluate the legality of the military conduct at issue.[344] Nonetheless, the court opined that the PCA and its implementing regulations derive from "the traditional American insistence on exclusion of the military from civilian law enforcement, which some have suggested is lodged in the Constitution."[345]

In *Dreyer*, the Ninth Circuit grappled with the PCA's constitutional underpinnings because such a determination was necessary before application of the exclusionary rule. The evolution of jurisprudence concerning the exclusionary rule is important here: it has been a traditional deterrent to unlawful surveillance. That question was avoided by the Fourth Circuit but necessarily decided by the Ninth Circuit. It will be front and center if military cybersurveillance or militarized cyberpolicing of civilians will be subject to judicial deterrents designed to protect the defendants in prosecutions deriving from such surveillance. And such defendants, like Dreyer, would typically be the most highly motivated and best-placed persons to identify and seek to remedy a PCA violation—so long as it meaningfully affects their own rights.

The outcome of *Dreyer* suggests that the military—or those acting under the auspices of the military—may be held accountable for deliberate cybersurveillance overreach, especially if they share incriminating information with civilian authorities. Although Fourth Amendment concerns about cybersurveillance operate in the background of *Dreyer*, it is clearly not a Fourth Amendment case. If civilian law enforcement engages in the use of RoundUp to monitor computers statewide, it is unclear that there would be any remedy by litigants—or jurists—seeking to deter this kind of governmental invasion of

340 490 F.3d 372 (4th Cir. 1974).
341 *Id.* at 373.
342 *Id.*
343 *Id.* at 375–76.
344 *Id.*
345 *Id.* at 376.

privacy. In short, here, a sympathetic Ninth Circuit panel found, in the PCA-like restrictions applicable to the Navy, the legal restraint needed to establish strong precedent about military use of this kind of cybersurveillance stateside. It remains unclear, however, after the Ninth Circuit's en banc decision whether such surveillance can be deterred outside the military context, given that the Ninth Circuit acknowledged a breach but denied any effective remedy.

Moreover, it is unclear if the Ninth Circuit opinion's attempt in *Dreyer* to establish a firewall between military and civilian surveillance is either legally practicable or realistic. The court objected to the scope of the search itself, not to what was done with the results. Pragmatically speaking, cybersurveillance, in this case through RoundUp, may be more efficient when done broadly because it might be easier to sift the civilian positive hits from the military positive hits of the search than to sort out the civilian computer addresses from the military computer addresses at the outset. Moreover, the court's holding seems to push against NSPD-59/HSPD-24, which seeks, for national security purposes, the "interoperability" of various federal agency data collection and storage methods.[346]

CONCLUSION

The Posse Comitatus Act of 1878, designed to limit the deployment of federal military resources in the service of domestic policies, may be ineffective as currently crafted and interpretted in light of the growth of cybersurveillance, and the adoption of cyberintelligence tools into day-to-day policing and governance functions. This Article describes a growing national bureaucratized cybersurveillance state that includes a host of technologies and government programs associated with the capture and analysis of biometric data. The military capture and use of biometric data, and the ways that it assists in the population management policies that are a component of current U.S. military operations abroad, deserves special attention.

Such operations do not, at this juncture, necessarily pose a Posse Comitatus Act problem. Rather, this Article attempts to explain the way military efficiencies in biometric surveillance may—and do—translate into population management techniques stateside. In such contexts, the Posse Comitatus Act will not provide the legal teeth scholars currently search for to bring Fourth Amendment privacy protections up to speed with current advances in techniques

346 Directive on Biometrics, *supra* note 32.

of data surveillance. Yet, when the federal, state, and local government and military may collaborate in the sharing and analysis of data that targets civilian populations at large, mass cybersurveillance risks attach and should be acknowledged and questioned. In other words, when data is commingled and used for dual purposes, military, foreign intelligence, and civilian law enforcement can no longer be separated practicably on a technological level, and the policies that mandate the Posse Comitatus Act may be threatened.

Maintaining strict separation of data between military and intelligence operations on the one hand, and civilian, homeland security, and domestic law enforcement agencies on the other, is increasingly difficult as cooperative data sharing increases. The Posse Comitatus Act and constitutional protections such as the Fourth Amendment's privacy jurisprudence, therefore, must be reinforced in the digital age to appropriately protect citizens from militarized cyberpolicing: the blending of military/foreign intelligence tools and operations with homeland security/domestic law enforcement tools and operations. This Article concludes that, as of yet, neither statutory nor constitutional protections have sufficiently evolved to cover the unprecedented surveillance harms posed by the migration of biometric cyberintelligence from foreign to domestic use.