2017

From the National Surveillance State to the Cybersurveillance State

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

ANNUAL REVIEWS

Annual Review of Law and Social Science

From the National Surveillance State to the Cybersurveillance State

Margaret Hu

School of Law, Washington and Lee University, Lexington, Virginia 24450;
email: hum@wlu.edu

Annu. Rev. Law Soc. Sci. 2017. 13:161–80

The *Annual Review of Law and Social Science* is online at lawsocsci.annualreviews.org

https://doi.org/10.1146/annurev-lawsocsci-110316-113701

This article is abridged with permission from Hu M. 2017a. Biometric surveillance and big data governance. In *The Cambridge Handbook on Surveillance Law*, ed. D Gray, S Henderson. Cambridge, UK: Cambridge Univ. Press. In press

Keywords

surveillance, cybersurveillance, big data, biometrics, National Surveillance State, national security

Abstract

This article anchors the phenomenon of bureaucratized cybersurveillance around the concept of the National Surveillance State, a theory attributed to Professor Jack Balkin of Yale Law School and Professor Sanford Levinson of the University of Texas School of Law. Pursuant to the theory of the National Surveillance State, because of the routinized and administrative nature of government-led surveillance, normalized mass surveillance is viewed as justified under crime and counterterrorism policy rationales. This article contends that the Cybersurveillance State is the successor to the National Surveillance State. The Cybersurveillance State harnesses technologies that fuse biometric and biographic data for risk assessment, embedding bureaucratized biometric cybersurveillance within the Administrative State. In ways that are largely invisible, the Cybersurveillance State constructs digital avatars for administrative governance objectives and targets digital data deemed suspicious. Consequently, constitutional violations stemming from cybersurveillance systems will be increasingly difficult to identify and challenge.

INTRODUCTION

This article addresses new developments in what has been termed the modern National Surveillance State (Balkin 2008, Balkin & Levinson 2006). The theory of the National Surveillance State situates the rise of the Cybersurveillance State within the Administrative State. This article argues that the political and technological structure that supports the emerging Cybersurveillance State is best examined through a theorization of the National Surveillance State. The political theory of the National Surveillance State is attributed to Professor Jack Balkin, Knight Professor of Constitutional Law and the First Amendment at Yale Law School, and Professor Sanford Levinson, W. St. John Garwood and W. St. John Garwood, Jr. Centennial Chair in Law, University of Texas School of Law. In the National Surveillance State, the governing emphases are on the following objectives: (*a*) a paradigm of preemptive action and preventive policing; (*b*) radically transparent identities often based on biometric data, purportedly to achieve better governing outcomes; and (*c*) technocratic policymaking and big data–driven decisionmaking that unfold in highly bureaucratized settings (Balkin 2008, Balkin & Levinson 2006). The infrastructure required to support these objectives is now often referred to as cybersurveillance architecture, a description that experts increasingly use for data surveillance (dataveillance), big data surveillance, and cybersurveillance (Granick 2017, Greenwald 2014a, Hu 2015b, Rosen 2005, Schneier 2015).

The exponential growth of cybersurveillance architecture and biometric identification systems is guided and mutually reinforced by these objectives. The coordinated rise of biometric surveillance and cybersurveillance governance systems is not coincidental but rather is due to the symbiotic relationship between the two (e.g., biometric cybersurveillance). In other words, technological developments have incentivized the biometric surveillance apparatus necessary to carry out precrime-governing rationales, identity management programs, and big data governance and decisionmaking systems—and vice versa (Balkin 2008, Balkin & Levinson 2006, Lyon 2009). At least on a theoretical level, the combination of big data surveillance methods and biometric surveillance systems allows for the analysis of nearly all computer-generated human information (Ingram 2013, boyd & Crawford 2012). These combined systems permit the collection, storage, and analysis of all digital footprints and data breadcrumbs. The consequence of this is that all individuals subject to such surveillance can be both biometrically and biographically tracked and assessed for risk.

Specifically, modern governance systems increasingly depend upon biometric identification technologies—e.g., scanned fingerprints and irises, digitized photos for facial recognition technology, and DNA—to anchor a person's physical identity to other biographical and behavioral data (Lyon 2009). Once a biometric identification anchor is established in a database, it can be used for other data-tracking activities, including data mining, database screening, digital watchlisting (Kahn 2013, Kalhan 2014, Scahill & Devereaux 2014, Shane 2007, Spiro 2014, Steinbock 2006), and automated "situational awareness" programs (Ramos 2014). In the years following the terrorist attacks of September 11, 2001, policymakers have pursued a preemptive approach to counterterrorism, and biometric identification and analysis systems play a part in that approach (Gates 2011, Hu 2013, Magnet 2011, O'Harrow 2005). Policymakers view these technological developments, including biometric technologies, as tools with the potential to identify individuals who may pose a threat to national and homeland security and to prevent crime and terrorism.

One example of technology intended for risk assessment and threat management is the post-9/11 program Total Information Awareness (TIA). TIA was the progeny of the Defense Advanced Research Projects Agency (DARPA) in the US Department of Defense. TIA can be understood as a "collect-it-all" data surveillance program. TIA was not explicitly identified as a collect-it-all program—this phrase originated with the Snowden disclosures. One National Security Agency

(NSA) slide described the NSA's procedure as "collect-it-all" (Greenwald 2014b). Collect-it-all efforts like TIA embody a philosophy that aspires to preventive policing. Mass data collection is construed as a tool to assess and prevent future threats (Murray 2010). In TIA and other programs tested or adopted after 9/11, biometric database screening and analysis have emerged as a preferred method for tracking, identifying, and establishing identity-based inferences in counterterrorism.

This article proceeds in three parts. The first contends that the Cybersurveillance State is overtaking the National Surveillance State through the capture of big data governance tools and philosophies that increasingly rely upon biometric surveillance as a form of identification and precrime risk assessment. The second part provides an overview of biometric identification technologies. This is intended to clarify the type of technologies discussed in this article. It also explains why biometric technology is a data backbone for other surveillance systems in governance strategies increasingly motivated by preventive policing. In a post-9/11 policymaking regime, more and more efforts are focused on preventing crime and terrorism before they occur. Biometric identification and identity assessments are becoming essential tools for multiple preventive purposes in criminal, military, and intelligence contexts. The third part addresses how precrime policy rationales are now informed by biometric-based analysis. In short, biometrics is the means by which analysis of a citizenry's data, and any resulting decisions based on that analysis, can be connected back to a physical person in the real world—whether to approve that person as eligible for a job, as some employment eligibility database screening systems like E-Verify are, by moving toward biometrics through adopting the E-Verify photo tool (Hu 2013), or to determine whether that person is eligible to fly on a commercial airline. The No Fly List and digital watchlisting systems are increasingly biometrically centered (Tau 2015). These types of governance assessments, however, fall within the civil law and administrative law structure. Biometric cybersurveillance systems can inform targeted killing decisions and other lethal consequences. Often in the service of precrime/counterterrorism policies, biometric cybersurveillance, therefore, is becoming a linchpin for broader policymaking and decisionmaking.

From the National Surveillance State to the Cybersurveillance State

Privacy law expert Neil Richards (2013, p. 1936) explains that "[w]e are living in an age of surveillance." Surveillance has transformed not only public governance but corporate and consumer governance through the emergence of what business scholar Shoshana Zuboff (2015, p. 75) calls "surveillance capitalism." The term surveillance has multiple definitions. The term cybersurveillance, however, has no agreed-upon definition. Law and technology scholar Lawrence Lessig (2006, p. 209) describes "digital surveillance" as "the process by which some form of human activity is analyzed by a computer according to some specified rule . . . . The critical feature in each [case of surveillance] is that a computer is sorting data for some follow-up review by some human." Digital media scholar Mark Andrejevic (2014, p. 56) describes a defining characteristic of "big data surveillance" as "the imperative . . . to monitor the population as a whole: otherwise it is harder to consistently and reliably discern useful patterns." Computer scientist Roger Clarke introduced the term dataveillance (Clarke 1988, p. 499; Lyon 2007), which he defines as the "systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons." Dataveillance provides a method by which all aspects of a person's life and identity may be transformed into digital data ready for analysis. David Lyon (2007, p. 16) clarifies the relationship between dataveillance and surveillance, explaining that "dataveillance also automates surveillance."

The normalization of continuous cybersurveillance is integral to the phenomenon of the National Surveillance State. Constitutional law scholars Jack Balkin and Sanford Levinson explain

that the National Surveillance State is driven by advances in technology (Balkin 2008, Balkin & Levinson 2006). It has a preoccupation with automated, transparent identities. It relies upon specific markers, such as social security and passport numbers, purportedly within a broader context of authentic governance objectives (Balkin 2008). Other scholars have explored the documents that constitute identity cards and the surveillance consequences of such documents (Harper 2006, Lessig 2006, Bennett & Lyon 2008, Lyon 2009, Sobel 2002, Strandburg & Raicu 2006). The Cybersurveillance State is dependent upon emerging developments in the big data cybersurveillance capacities of both the public and private sectors (Hu 2015c). Scholars have explained that big data is predictive and correlative (Citron & Pasquale 2014, Pasquale 2016, Richards & King 2013) and can be seen as a form of artificial intelligence (AI) or machine learning (Mayer-Schönberger & Cukier 2013). Big data depends on a never-ending supply of digital data that informs computer-generated conclusions (Mayer-Schönberger & Cukier 2013).

> Though it is described as part of the branch of computer science called artificial intelligence, and more specifically, an area called machine learning, this characterization is misleading. Big data is not trying to teach a computer to think like humans. Instead, it is about applying math to huge quantities of data in order to infer probabilities. (Mayer-Schönberger & Cukier 2013, pp. 11–12)

Big data developments transform governance philosophies, such as the adoption of precrime governance strategies. The Cybersurveillance State is now poised to overtake the National Surveillance State through the capture of big data governance tools and philosophies that increasingly rely upon biometric identification and precrime assessment tools. A governance philosophy that relies on isolating and analyzing biometric and biographical data—what privacy scholar Julie Cohen (2015) refers to as legal constructs under a "biopolitical public domain"—operates under the assumption that big data and biometric technologies have infinite efficiency-enhancing capacities. The National Surveillance State's capture of its citizenry's data trails to regulate and police the big data state runs parallel with the corporatization of personal data. Big data has transformed both the public and private market into a political and information economy in which an individual can be reduced to a digital profile made up of data points that can be subjected to surveillance, analysis, and exploitation (boyd & Crawford 2012). Mayer-Schönberger & Cukier (2013, p. 157) contend that "the new thinking is that people are the sum of [the data]." Their concern is that

> because the government knows whom it will want to scrutinize, it collects, stores, or ensures access to information not necessarily to monitor everyone at all times, but so that when someone falls under suspicion, the authorities can immediately investigate rather than having to start gathering the info from scratch. (Mayer-Schonberger & Cukier 2013, p. 157)

Daniel Solove (2002) describes "digital dossiers," which aggregate information to assemble a complete profile of an individual. The combined power of multiple technological innovations that collect and fuse biographic data and biometrics and track digital footprints can be used to create digital avatars (Hu 2015c). These avatars are an outgrowth of the Cybersurveillance State's policies of radical identity transparency and permit analyses of a population's data and data connections among subpopulations for suspicious indicators.

Biometric surveillance is an integral component of the big data age in both governance and economic developments. Biometric surveillance is integrated into the Internet of Things, for example, the network in which "objects in your house, car, office, and smartphone communicate, interact, report, track, and provide vast amounts of data about the activities of their owners"

(Ferguson 2016, p. 807; Friedland 2015). Under the National Surveillance State, governance in the big data world means the collection and monitoring of the citizenry's data trails to facilitate government benefits and policing. In a world in which daily data trails are increasingly monitored and collected by public and private watchers, biometric data serve as a means to tie physical and behavioral data points to other digital data. To do so, biometric data must be digitally captured. Once in digitized form, biometric data can be aggregated with other biometric databases and assimilated into biographic databases.

The big data revolution is just beginning. Because datafication is in its infancy, the cybersurveillance capacities of big data governance systems, like the No Fly List, are still in nascent stages. Datafication, like most big data processes, requires increasing amounts of digital data to support or construct cybersurveillance. It empowers government actions that are based on digital data collection, data processing protocols, and bulk data analyses (Mayer-Schönberger & Cukier 2013). Another way to characterize datafication is as a governmental policy interest that both transforms analog data (PCAST 2014) into searchable, centralized digital databases and develops new forms of stored data.

New surveillance methods and varieties of datafication make it possible for the government to infer a suspect's status by fusing locational and biographical-behavioral surveillance. This process facilitates identity verification and data management protocols that permit tracking and analytics for a variety of tasks, including identifying potential suspects or inferring terroristic characteristics. The 2014 White House Report to the President from the President's Council of Advisors on Science and Technology (PCAST 2014), titled *Big Data and Privacy: A Technological Perspective*, is useful for understanding the fusion process that is made possible through big data. The PCAST report described the private sector consumer fusion processes in the following manner:

> Data fusion occurs when data from different sources are brought into contact and new facts emerge. 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. (PCAST 2014, p. x)

Surveillance of an individual's body can be fused with biographical surveillance through big data tools. The process of biometric datafication refers to transforming an individual's physical and behavioral characteristics into data (Mayer-Schönberger & Cukier 2013). Datafication of an individual's body in a big data governance system occurs first through the capture of geolocational and biometric data. Next, the data is aggregated, stored, and analyzed.

The 2014 White House PCAST (2014) report recognizes the potential role of fusion in government data analytics. Fusion can predict an individual's perceived threat level in criminal and terrorism investigations. Programs such as Social Radar, for example, can use fusion to identify perceived threats from social and political movements, including classifications of individuals and what has been referred to as "social contagions" (Ahmed 2014). Former Chief Scientist of the US Air Force Mark Maybury is publicly attributed as the primary architect of Social Radar (Shachtman 2012). An AI and language processing specialist, Maybury has explained that the US Department of Defense is currently attempting to construct "a virtual sensor, combining a vast array of technologies and disciplines . . . [as] part of a broader Pentagon effort to master the societal and cultural elements of war" (Shachtman 2012). In other words, "using biometrics, Social Radar

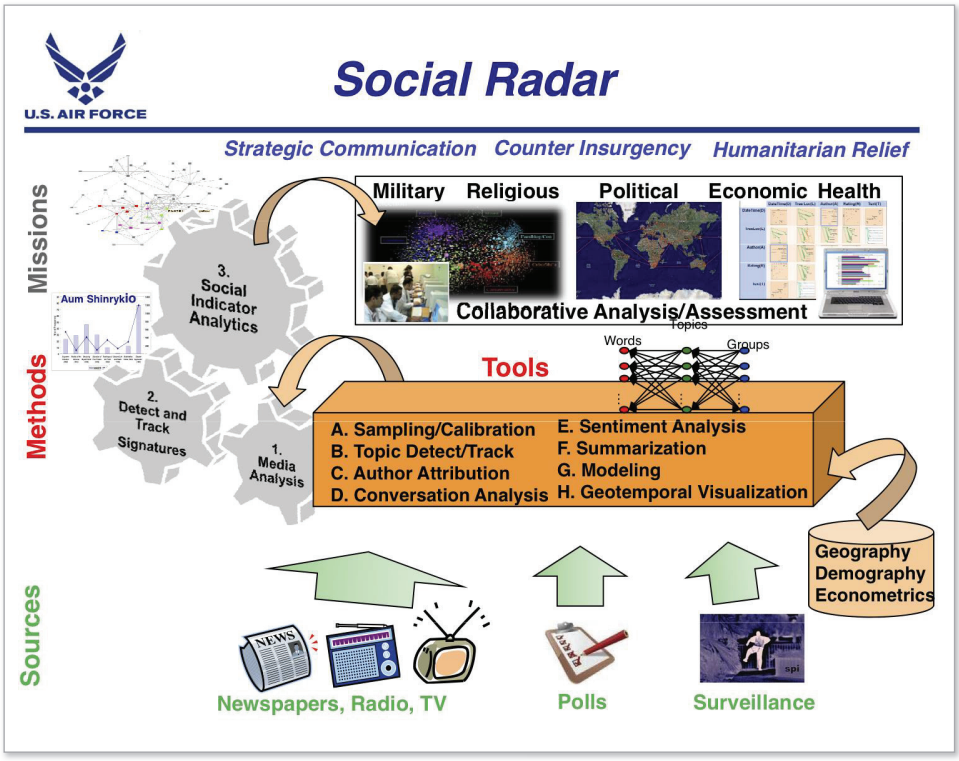

Figure 1

Social Radar (project of the US Department of Defense, US Air Force). Figure copyright © 2010 from Maybury M. 2010. Cross-cultural decision making. In *Social Radar for Smart Power*, ed. D Schmorrow & D Nicholson. Boca Raton, FL: CRC Press. Reproduced by permission of Taylor and Francis Group, LLC, a division of Informa plc.

will identify individuals . . . . Using sociometrics, it will pinpoint groups. [Sociometric datapoints include] Facebook timelines, political polls, [and] spy drone feeds" (Shachtman 2012). As of 2012, the Pentagon had invested over $125 million to "quantify, model—and, eventually, foresee—the human, social, cultural, and behavioral dimensions of conflict" (Shachtman 2012).

Figure 1 provides a pictorial depiction of the comprehensive cybersurveillance anticipated through the Social Radar system, which anticipated the full integration of drone footage, biometric data signatures, econometrics, and other intelligence sources to achieve higher-order cybersurveillance inferences.

Social Radar appears to trace its philosophical origins to TIA. The development of TIA after the 9/11 terrorist attacks was guided under the leadership of the newly created Information Awareness Office within DARPA (Harris 2012, Murray 2010). Within this office, TIA was an effort led by retired Navy Vice Admiral John M. Poindexter (Murray 2010), who served as a national security advisor to President Reagan (Harris 2012). TIA was informed by a philosophy of "predictive policing," which "focuses not on collecting evidence about actual wrongdoing but on the broad collection of information about everyday activities with the intention of detecting (and preventing) future behavior" (Murray 2010, p. 5). Congress officially defunded TIA in late 2003 (Murray 2010, Slobogin 2008, *USA Today* 2003). Experts have nonetheless noted that remnants of the TIA program and its philosophy have persisted. Even prior to the 2013 disclosures by Edward Snowden,

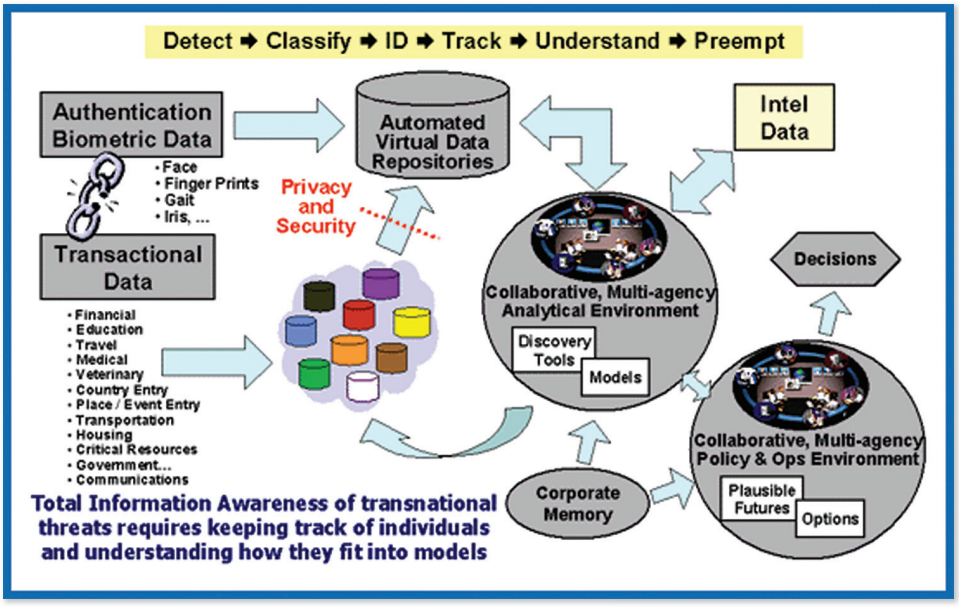

Figure 2

Total Information Awareness (TIA) (former project of the US Department of Defense, DARPA) (TruthMove 2016).

experts had explored the possibility that the NSA had constructed a global surveillance apparatus that shared TIA's goals (Harris 2012, Murray 2010, Slobogin 2008). Specifically, in an interview, computer scientist David J. Farber, often referred to as the Grandfather of the Internet, opined that TIA had carried on within the NSA and that evidence of TIA's quiet existence is visible in the types of programs disclosed by Edward Snowden (Horgan 2013). Over the past decade, there has been growing interest in surveillance systems (Slobogin 2014). This attention has revealed various programs that appear to duplicate TIA's ambitions of using bulk data and digital dossiers to prevent future acts of crime and terrorism. Other programs have the goal of predicting "social contagions" by collecting and analyzing social media and internet activity (Ahmed 2014).

Poindexter (2002) has explained that TIA was designed to "detect, classify, identify, and track terrorists so that we may understand their plans and act to prevent them from being executed." The collect-it-all cybersurveillance effort was aimed beyond the intelligence community; as Poindexter (2002) stated, "in the case of counter-terrorism, it is broader to include law enforcement, friendly allies, outside experts, etc." **Figure 2** provides a graphic depiction of how TIA was intended to operate.

As **Figures 1** and **2** show, biometric data appear to be a data backbone that provides a source for the evolution of multiple identity screening systems. This biometric backbone is analogous to the manner in which social security and passport number systems form a numerical data backbone for database screening. The cybersurveillance sweep of the data of entire populations and subpopulations requires a method to isolate individuals within that population or subpopulation for more isolated targeting and further investigation. Biometric data can serve this purpose, as demonstrated by the portion of TIA's **Figure 2** referencing "authentication [of] biometric data." Authentication of biometric data—specifically face, fingerprint, gait, and iris scans—suggests that identity verification and identity determination can be executed through biometric database screening.

One of the biometric data programs under TIA, for instance, referred to a component known as "Human Identification at a Distance," meant to "achieve positive identification of humans using multimodal biometric technologies" (Poindexter 2002). The manner in which multimodal biometric data—a combination of biometric identifiers, such as facial recognition technology and iris and fingerprint scanning—can serve predictive policing purposes by anchoring one's identity is demonstrated by TIA's reference to "authentication [of] biometric data" in a DARPA infographic slide (TruthMove 2016). Authentication of biometric data—with the TIA slide specifically listing examples of biometric identifiers such as face, fingerprint, gait, and iris scans—suggests that identity verification and determination can be executed through biometric database screening.

TIA, Social Radar, and other collect-it-all programs with precrime governing ambitions are able to maximize technological capacities in a way that can permit the cybersurveillance monitoring of entire populations to pinpoint suspicious data profiles. This monitoring can take the form of digital watchlisting and database screening systems that isolate data, devices, or persons deemed suspicious, for instance, or other data tracking or data surveillance methods. The Snowden disclosures and other media reports appear to confirm that suspicious data, rather than suspicious persons, are targeted (Scahill & Greenwald 2014). For example, a former drone operator for the US military's Joint Special Operations Command explained that NSA drone strike targets are often identified through metadata analysis and cell phone tracking. He explained, "It's really like we're targeting a cell phone. We're not going after people—we're going after their phones in hopes that the person on the other end is a bad guy" (Scahill & Greenwald 2014). For strikes seeking greater precision, once a data profile is isolated and deemed suspicious, biometric data may serve as a means to isolate the individual associated with that profile, such as voice recognition (Poitras et al. 2014).

As a result, the Cybersurveillance State, as a technological successor to the National Surveillance State, will execute bureaucratized biometric cybersurveillance in ways that are largely invisible and that appear routinized when technologically embedded within biometric identification technologies harnessed by the Administrative State. The normalization of day-to-day cybersurveillance will be achieved largely through governing functions that appear purely administrative (e.g., identity assessments for the granting of welfare, rights, privileges, and governing incentives). Because of the routinized and administrative nature of the government-led big data program or data surveillance (dataveillance) program, contemporary cybersurveillance is likely to be viewed as justified under crime, immigration control, and counterterrorism policy rationales.

Overview of Biometric Identification and Verification Technology

Currently, biometric verification and identification technologies are not commonly perceived to be surveillance technologies—the public and private sectors typically treat them as a benign and useful form of digitized identification. Such automated biometric screening is considered to be a more efficient form of small data verification technologies, such as human screening or human-driven practices involving assessments of biometric or forensic data. Small data biometric verification could include comparing a passport photo against the person holding the passport. Big data biometric identification, however, has a distinct impact from that of small data biometric investigation because it can facilitate surveillance. Big data photo screening may entail the collection of digital photographs. This in turn can lead to facilitating facial recognition technology through the mass digitization of photo databases, potentially including billions of facial images. One Snowden disclosure noted that the NSA collects millions of digital photographs from internet and social media sources and uses facial recognition technology to identify individuals (Risen & Poitras 2014). Big

data identification systems rely on algorithmic, database-driven facial recognition technology that enhances the capacity for mass surveillance capacities in ways that are difficult to understand.

The potential for mass surveillance is part of the problematic nature of biometric credentialing and identification practices. Like most digital data, biometric identification data are not restricted to the purpose for which they were originally collected. Biometric data can be repurposed for secondary uses, such as identification of potential suspects or victims through real-time analytics, assessment of threats of terrorism, tactical decisionmaking, or behavioral and genetic research (Duster 2003). Beyond secondary—and tertiary, quaternary, and quinary—uses, biometric data become a part of population-wide risk assessments that incorporate bureaucratized surveillance into governing decisions, policing, and threat assessments. Through big data tools, precrime governance models are increasingly reflected in collect-it-all cybersurveillance systems. In these systems, biometric data is a surveillance axis that can be used to track, identify, and isolate suspicious persons, digital data, or devices (Hu 2015a).

As a result of big data biometric governance trends, meaningful distinctions between biometric credentialing for identification and behavioral biometric profiling are disappearing. The objectives are merging: Reliable credentialing is used to advance security and precrime policy rationales. Biometric data mission creep occurs by necessity in a big data world because the cybersurveillance systems are often designed to engage in mass data integration and analysis and predictive policing. Biometric surveillance serves two purposes in preventive policing: It increases identity transparency, and the biometric data categorize identity through cataloging behavioral and physical characteristics and assess these characteristics for risk.

Contrasting small data biometric credentialing protocols with big data credentialing protocols is useful. It illustrates how biometric surveillance fits within the Cybersurveillance State. In a small data world, paper-based passports and nondigitized photographs are examples of a small data biometric-based identification system. In a big data world, a digitized passport system can link to multiple other sources, such as license plate readers, No Fly Lists, and Terrorist Watchlists. Facial recognition technology drawing upon a photo database could potentially link a plethora of digital images of a person, including social media, the internet, photo databases like driver's licenses, live-streaming video, CCTV surveillance, and images obtained from hacking cameras on laptops and digital devices. Biometric data collection and storage are becoming increasingly compulsory through either government identification requirements, such as digital photo requirements for passports and driver's licenses, or corporate identification requirements, such as biometric access to digital devices.

Because of technological developments and trends in governance, it is challenging, if not impossible, to prevent biometric data capture and collection. Biometric surveillance systems increasingly require opting in as the price of social, economic, and political participation. Biometric data capture is difficult to resist because it is simultaneously compulsory and transparent. Biometric data collection is often compulsory because it is increasingly mandatory to establish identity. Biometrics are transparent qualities because it is very difficult to hide biometrics; an individual's face, iris, or fingerprint can be digitally captured in any public place. Because biometric data support larger big data programs, such as No Fly List–type risk assessments, it is extraordinarily difficult, if not impossible, to opt out (Hu 2017a).

Biometrics is "[t]he science of automatic identification or identity verification of individuals using [unique] physiological or behavioral characteristics" (Vacca 2007, p. 589). Biometric-based identification can involve collection and analysis of hard or primary biometrics (Vacca 2007): traditional biometric data identifiers that support automated identity verification technologies. Examples include scanned fingerprints, facial recognition technology, iris scans, and DNA database

screening. Automated biometric data systems serve "secure identification and personal verification solutions" (Vacca 2007, p. 57).

Biometric-based identification or identity verification systems may also collect and analyze "soft biometrics," or secondary biometrics (Niinuma et al. 2010). Soft biometrics are distinguished from hard biometrics based on their perceived reliability in automated identification characteristics. Soft, or secondary, biometrics is defined as an "anatomical or behavioral characteristic that provides some information about the identity of a person, but does not provide sufficient evidence to precisely determine the identity" (Li & Jain 2009, p. 1235). Examples of soft or secondary biometric identification systems include digital analysis or automated determination of age, height, weight, race, ethnicity, hair and skin color, scars and birthmarks, and tattoos (Li & Jain 2009). Behavioral biometric data are defined as "traits that are learned or acquired" (Vacca 2007, p. 3). Biometric behavioral identifiers include a range of traits such as keystroke patterns and mouse-use characteristics; analysis of gait and signature; voice identification; and cognitive biometrics, such as neural responses. Other biometric identifiers might include skeletal bone scans, brain scans, body odor, eyebrow shape, and ear shape. Some biometric data may be combined with verifying data to infer information about an individual. This other biometric data could include heart rate, perspiration, sweat pore analysis, and eye pupil dilation.

Digitized biometric identification and biometric database screening technology aims to remove human decisionmaking from the matching process. Instead, matching is done by an automated or semiautomated system. Biometric technology is increasingly considered by the political branches to be an efficacious policy prescription for complex homeland security, national security, immigration control, and intelligence or military matters (Hu 2017a). The political branches perceive biometric data as the gold standard of identity management systems: It is presented as scientifically objective and purportedly forgery proof through algorithmic analysis (Garfinkel 2000, Gates 2011, Hu 2013, Lynch 2012, Magnet 2011). A similar algorithmic identity management system, E-Verify, now operates to verify identity before authorizing the right to work. Although E-Verify does not currently require a biometric identification component, it has been discussed in Congress (Hu 2013, Ries 2010). It affects the right to drive: The Real ID Act of 2005 [Pub. L. No. 109–13, 119 Stat. 302 (codified as amended in scattered sections of 8 U.S.C. 2012)] includes technological enhancements and requires digital photos that can be analyzed with facial recognition software. It also potentially affects the right to vote [42 U.S.C. § 15483(a) (2012); US Gov. Account. Off. 2010]. These verifications are purportedly to more effectively secure the border and screen out potential terrorist threats, criminal aliens, or unlawfully present immigrants. Many of these identity management systems are moving toward biometric data as a method for identity verification.

Once biometric data have been collected, to make identity screening feasible, the data must be compiled within a database. Using biometric data for identity verification and authentication supports Department of Homeland Security's (DHS) domestic identity management goals (Cyber Sec. Res. Dev. 2016, Thomson 2007) and the Department of Defense's international population management goals (*Public Intelligence* 2014). DHS defines identity management as including administrative processes that serve "authentication and authorization" goals through managing technological, facilities, and digital data access (Cyber Sec. Res. Dev. 2016). Identity management mediates "user rights, entitlements, and privileges with the established identity" (Cyber Sec. Res. Dev. 2016).

The US military used the term population management in relation to international security to describe a broad category of goals considered essential to achieving strategic military objectives. For example, the term population management serves to operationalize and explicate the justification for the data collection of the biometrics and "contextual data" of "every living person in Afghanistan," which has been identified as a US military objective (*Public Intelligence* 2014).

Acquisition of biometric surveillance technologies and biometric databases is a common government practice to facilitate governance goals. Day-to-day uses include criminal and counterterrorism purposes: counterterrorism, military, or intelligence identification, homeland security, border security, immigration control, and criminal identification or surveillance. Tools in these programs include fingerprint and facial recognition technology using database screening, prison visitor systems, and parole monitoring. Other biometric surveillance technologies may be used in civil identification, such as drivers' license or voting systems or benefit-payment systems, for example, biometric identification as a condition for obtaining welfare benefits. Biometrics can also be deployed to restrict access to physical locations (physical access) and technological access (logical access). Logical access restrictions may include measures such as requiring biometric IDs before accessing computer and electronic devices and internet services. Such restrictions expand data collection and analysis capacities and provide more accurate digital avatars that in turn support the Cybersurveillance State's mission of complete identity transparency (Hu 2013).

In other words, government-led biometric surveillance is often for the purpose of identification and identity-based assessments: verification of identity (Is this person who they claim to be?), determination of identity (Who is this person?), and identity-based assessments (Does this person have a criminal or terroristic disposition?). The process of biometric identification may, but does not necessarily, involve traditional surveillance activities, such as domestic or foreign intelligence gathering. Advances in biometric surveillance represent a new era of cybersurveillance. Under cybersurveillance technologies, governing emphasis is placed on big data–driven protocols: mass data collection and aggregation, data mining and database screening, digital watchlisting, algorithmic intelligence, and risk assessment and predictive analysis.

Biometric surveillance can involve the following types of activities in combination or standing alone: capturing, storing, and tracking biometric data; aggregating, databasing, and sharing biometrics; and analyzing biometric identifiers (Biometric Information Privacy Act, 740 Ill. Comp. Stat. 14). Biometric surveillance as a form of bureaucratized surveillance is not new. For example, the compilation of photographs by police into record books to help identify suspects, files consisting of passport photographs compiled for the purposes of identification, and even the Federal Bureau of Investigation's national fingerprint and DNA databases are established forms of biometric surveillance.

However, biometric cybersurveillance is new, as are big data system–dependent forms of governance (Wittes & Blum 2015). Examples of bureaucratized biometric cybersurveillance may include digitized, biometric-based social security cards or passports. A 2010 immigration reform proposal from senators Schumer & Graham (2010) recommended adopting a high-tech social security card that can be swiped like a credit card. This digitized biometric card could replace the numeric, paper-based social security card (Schumer & Graham 2010). Biometric databases assembled to implement such a card could then enable surveillance to identify individuals and aggregate data, such as where and when the credentials were presented.

Adoption of new technologies such as these will only expand trends in biometric surveillance and big data governance. As discussed below, adopting biometric-based identification systems will likely lead to long-term surveillance consequences. Digitized and machine-readable identification documents that can collect and aggregate data in databases risk feeding comprehensive and interrelated cybersurveillance systems (e.g., Total Information Management and collect-it-all systems).

The merger of biometric surveillance with big data tools—what can be described as biometric cybersurveillance or biometric identification cybersurveillance—can dramatically expand the cybersurveillance capacities of governments. A government-administered identification system has the capacity to make its biometric data collection protocols compulsory, or near-compulsory, by

conditioning government privileges and benefits on compliance with biometric data collection. For example, a digitized biometric-based identification system—such as a biometric database screening system to establish identity for employment, voting, flying, or driving—could enable the development of a near-universal biometric database.

Such a centralized database could have multiple functions, including identity verification and identity tracking. This database would potentially contain a wealth of uniquely identifying information on a heretofore unknown scale. Further, the data could be combined or exchanged with other databases. Possible analyses through cross-referencing would be infinitely enlarged. The potential inferences of suspicion that could be drawn in identity assessments would be infinitely augmented. As stated above, big data is predictive; thus, these identity-based bureaucratic systems could serve precrime goals.

Biometric verification technologies are commonly used in the private sector as well, particularly for restricting technological access, such as fingerprint readers on smartphones; facial recognition technology for laptops; or logical access restrictions, which limit an individual's ability to access technology, the internet, telecommunications, or ATMs (Hu 2013). Biometric verification may restrict or grant physical access, such as biometric-enhanced security measures at Walt Disney. Some employers have begun inserting microchips into employees' bodies that can unlock doors, operate electronic equipment, or make purchases (Assoc. Press 2017). Private sector biometric data is increasingly available to governments, as demonstrated by law enforcement access to private DNA databases used for familial and genetic historical information (Koerner 2015).

The ability to combine biometric databases with public and private databases makes precrime and preterrorism objectives appear more plausible in the eyes of policymakers. Precrime governing ambitions that once could only be imagined in science fiction are now perceived as within the realm of possibility with the aid of biometric-based identity management systems and other comprehensive cybersurveillance systems that try to combine 24/7 body tracking with 360° biographical tracking. Predictive policing relies on big data tools and algorithms, methods of analyzing mass data collection to assess future risk. Although multiple experts challenge the validity of precrime programs (Ferguson 2015, Furnas 2012, Mayer-Schönberger & Cukier 2013, O'Neill 2016) and explore the limits of biometric surveillance (Garfinkel 2000, Gates 2011, Lynch 2012, Magnet 2011), precrime policy rationales are increasingly behind the drive to adopt biometric surveillance technologies and other cybersurveillance systems.

Biometric data surveillance thus differs from other types of data surveillance. Biometric data are privileged in the development of cybersurveillance regimes. This is because biometric data anchor identity-based data points for the purpose of connecting identity data to other data points. This process can also serve as a means of enabling bureaucratized and automated or semiautomated decisionmaking. Thus, collection and analysis of biometric data are involved in a multitude of public and private services. These include, for example, border security, including biometric data harvesting and analysis at points of entry; cybersecurity safeguards, including password protection and user identification (Apple Inc. 2016, Schneier 2016); and attempts to discover possible motives or threat-related behaviors in risk assessment protocols.

The use of biometric data for security purposes is alluring because, as the data come from an individual's body, it is often considered forgery resistant (Yakowicz 2016). Digitized biometric data provide a unique technological identifier that is obtained from an individualized characteristic of a person's body (Pato & Millett 2010). Biometric data can be pulled, for example, from digital photographs and voice recordings that are then processed by facial and voice recognition technologies (Pato & Millett 2010, Vacca 2007). Law enforcement and other government agencies consider biometric-based surveillance technologies effective because they can be multipurpose surveillance tools. For example, there are systems that combine facial recognition technology with automated

license plate readers (Shockley 2014). Other emerging biometric surveillance technologies, described as situational awareness surveillance systems, are sensor-network oriented. These systems can integrate biometric surveillance, such as facial recognition, with live-streaming video, real-time social media, and other surveillance screenings (Faraone et al. 2014, Garvie et al. 2016). Because biometric identification technologies can integrate into social media and internet screening, governmental precrime and preterrorism ambitions are increasingly linked to biometric surveillance capacities.

The popular assumption is that biometric identification credentialing is among the most secure, reliable, and technologically advanced. Although biometric data are understood to set the gold standard for identification systems (Gomez 2013), such identity tools are not without their flaws: They have proven vulnerable to hacks and may be less secure than traditional password protection (Murgia 2016). Thus, arguments challenging the infallibility of biometric identification sound counterintuitive. Biometric data's reputation as the gold-standard identification method originated in a small data world. In that world, biometric data verification was combined with human judgment and perception and forensic science applications (Hu 2015c).

Yet, in a big data world, biometric data are increasingly vulnerable and carry greater potential for fraud and abuse. It is the digitization of biometric credentialing and screening that makes it more vulnerable. In a big data world, algorithms and supercomputing tools are considered superior to small data forensics or human judgment and perception. Thus, digitized forms of exploitation can weaken the security and reliability of big data biometric credentialing because it is possible to manipulate these tools or the underlying biometrics. Digitized images and internet data trails permit biometric data to be hacked, rigged, spoofed, stolen, and duplicated (Fox-Brewster 2015, Hern 2014, Hu 2017a).

Biometric password protection for digital devices such as smartphones is often presented as tamper resistant. Researchers, however, have revealed vulnerabilities in biometric identification methods. Computer scientists have been able to spoof mobile fingerprint readers to unlock fingerprint recognition systems (Cao & Jain 2016). In one instance, local law enforcement sought the expertise of these scientists to gain access to a homicide victim's fingerprint password–protected smartphone. Law enforcement provided the scientists with the victim's fingerprints, which the scientists used to produce enhanced 2D fingerprints that could unlock the phone (Jesse 2016). Facial recognition technology and retinal recognition, often presented as necessary for identity security, are similarly vulnerable. Security and computer vision specialists in one study were able to create a digital 3D facial model using publicly available photos that deceived four out of five authentication systems (Newman 2016). In another study, a research team relied upon iris codes in security databases to recreate synthetic irises that, according to the researchers, successfully passed recognition tests 80% of the time (*BBC News* 2012).

Precrime Policy Under Biometric Surveillance and Big Data Governance

In the previous sections, the discussion focused on the aggregation of biometric data and other data. In a big data world this aggregated data can be filtered through multiple systems: databases, screening, digital watchlisting, and other dataveillance and cybersurveillance programs. Data screening technologies can pinpoint sources of suspicion, and biometric technologies can then identify specific individuals linked to the digital avatar or technological surrogate, such as a smartphone, that is the target. This section focuses on the administrative and bureaucratized nature of biometric surveillance technologies that can inform governmental actions that potentially can range from "being temporarily detained to deportation, prison, or death" (Dep. Homel. Secur. 2008, p. 2).

The recent Snowden disclosures of NSA cybersurveillance programs and other media reports appear to indicate that biometric data (Risen & Poitras 2014), if and when it is fully integrated into other dataveillance systems, may inform targeted killing technologies (Gellman & Soltani 2013, Miller et al. 2013, Scahill & Greenwald 2014). The Snowden disclosures revealed that drone strikes "rel[y] heavily on the NSA's ability to vacuum up enormous quantities of email, phone calls and other fragments" (Miller et al. 2013). Information provided in the Snowden disclosures suggested that harvesting and fusion of biometric and biographic data from digitized sources, including social media and the internet, were likely used for intelligence purposes. From one of the Snowden documents, the NSA states one goal as to "'compile biographic and biometric information' that can help 'implement precision targeting'" (Risen & Poitras 2014). "Targeting," although not defined in this particular Snowden disclosure, is a specific term of art. It can frequently refer to targeted killing measures and drone strikes (US Dep. Def. 2011).

Prior to the Snowden disclosures, media reports suggested that the US military is awarding contracts to defense contractors tasked with developing the integration of biometric data into targeting technologies (Shachtman 2011). These technologies are intended to be both analytic and predictive. For example, the Adversary Behavior Acquisition, Collection, Understanding and Summarization (ABACUS) tool would "integrate data from informants' tips, drone footage and captured calls" to "apply 'a human behavior modeling and simulation engine'" (Shachtman 2011). Many of these systems are driven by databases. For example, a database referred to as the disposition matrix that was developed under the Obama administration "is designed to go beyond existing kill lists, mapping plans for the 'disposition' of suspects beyond the reach of American drones" (Miller 2012). These emerging big data cybersurveillance systems integrate mass biometric dataveillance technologies into other intelligence data to identify potential terrorists or other security threats.

Other Snowden disclosures appeared to reaffirm the value of biometric surveillance to the intelligence community as a tool that could inform "precision targeting" decisionmaking, including, for example, attempting to increase the accuracy of intelligence to inform drone strikes (Risen & Poitras 2014). The intelligence community is increasingly reliant upon biometrics to identify targets and suspicious behavior through the analysis of unique physiological and behavioral characteristics. For example, one 2010 NSA document explains, "It's not just the traditional communications we're after: It's taking a full-arsenal approach that digitally exploits the clues a target leaves behind in their regular activities on the net to compile biographic and biometric information that can help implement precision targeting" (Risen & Poitras 2014).

Yet it is important to note that many biometric surveillance technologies and cybersurveillance systems—along with the data they capture and the findings they produce—are highly experimental. There is a risk that technologies might be rolled out prematurely and that biometric identification will be abused through mission creep: Identity verification programs pose a threat of drifting into TIA-type mass surveillance systems that may inform a broad range of predictive inferences (Hu 2017a). The routinization and bureaucratization of cybersurveillance through daily governance functions ensure the invisibility of this mission creep, especially the migration of military surveillance and foreign intelligence technologies to domestic use and daily law enforcement (Balkin 2008, Hu 2017b). These cybersurveillance technologies algorithmically fuse data to assess risks and threats. A military contractor explained that one biometric fusion program, Clear Heart, although intended for US military use, was adaptable to domestic use, including "'domestic security, border protection and state and local law enforcement . . . . envision[ing] a host of uses for this anywhere there is a need for crowd control, antidrug, anticrime and border control'" (Modus Operandi 2012).

This mission creep is facilitated by fully transparent identities made possible by universal biometric databases from the public and private sectors. The Snowden disclosures and other reports

explain how, in the Cybersurveillance State, biometric data operate as a foundational surveillance anchor point. Biometric data analysis in national security contexts is becoming ubiquitous. "While once focused on written and oral communications, the NSA now considers facial images, fingerprints and other identifiers just as important to its mission of tracking suspected terrorists and other intelligence targets, the documents show" (Risen & Poitras 2014). NSA documents disclosed by Snowden explain that the agency intercepted millions of digital images daily, including "about 55,000 'facial recognition quality images'" (Risen & Poitras 2014). It was also revealed that facial recognition technology was applied to digital photographs obtained from the internet and used to identify an individual. This biometric identification was screened against "two dozen data points" that included the "Transportation Security Administration no-fly list, [the individual's] passport and visa status, known associates or suspected terrorist ties, and comments made about him by informants to American intelligence agencies" (Risen & Poitras 2014).

Biometric surveillance is increasingly common in domestic contexts. A 2016 report by the Georgetown Law Center on Privacy and Technology noted that law enforcement facial recognition networks include over 117 million American adults, and at least 26 states permit law enforcement to search against drivers' license photos (Garvie et al. 2016, p. 2). In a small data world, intelligence and law enforcement collected and analyzed small data—written and oral communications. In a big data world, biometric data collection serves to identify and anchor data points around the individual to allow inferences of suspicion. The National Surveillance State, and now the emerging Cybersurveillance State, incentivizes a merger between foreign and domestic biometric intelligence gathering and corporate biometric surveillance (Hu 2017b, Strahilevitz 2012). Increasingly, the data collected by the National Surveillance State is used for cybersurveillance purposes. The Cybersurveillance State intentionally and inadvertently captures data that is a byproduct of datafication (Mayer-Schönberger & Cukier 2013). Inferences of suspicion in the Cybersurveillance State rely on both primary and incidental data (e.g., secondary and tertiary data).

The National Surveillance State poses problems that existing legal structures do not anticipate and may be unable to resolve (Balkin & Levinson 2006). Balkin (2008, pp. 15–16) explains that in the National Surveillance State, the danger is that "government will create a parallel track of preventative law enforcement that routes around the traditional guarantees of the Bill of Rights," and that "traditional law enforcement and social services will increasingly resemble that parallel track." In the Cybersurveillance State, individuals will be increasingly unable to identify the rationales behind being digitally blacklisted and unable to challenge the consequences of presumption of data-derived guilt (Citron & Pasquale 2014, Hu 2015a, Pasquale 2016). Balkin & Levinson (2006) have explained that the procedural protections set forth by the Constitution are insufficient in the National Surveillance State. Laura Donahue (2012) and other experts have concluded that neither surveillance law nor privacy statutes, nor the Fourth Amendment of the United States Constitution, are sufficient. As a consequence, further legal protection is necessary in the face of new types of surveillance harms stemming from emerging biometric data identification and tracking technologies.

Although the government embraces mass biometric-based identification systems, there has not been a sufficient analysis of due process protections for individuals subjected to biometric identification systems (Pato & Millett 2010). An individual wrongly identified through one of these systems may not be able to interrogate the chain of evidence relied upon or contest the databases or algorithms that have reached the erroneous conclusion (Kaye 2013, Mnookin 2010, Murphy 2013, Roth 2010). Nor is there a federal regulatory body that establishes and supervises standards for biometric data and technology. The National Institute of Standards and Technology (NIST) is tasked with testing oversight of federal biometric technologies, but NIST does not set

minimally proficient standards (US Gen. Account. Off. 2002). As a result, the Cybersurveillance State grows unchecked: The more data is collected, the more data is analyzed, the more data is generated from the analysis, and the more data is required. Because of a greater emphasis on identity transparency and identity management, the National Surveillance State is becoming a Biometric Cybersurveillance State.

CONCLUSION

The Cybersurveillance State, like the National Surveillance State, normalizes surveillance through the Administrative State. In contrast to the National Surveillance State, however, it will emphasize the need to govern data selves and manage threat risks attached to digital avatars rather than the need to govern individuals. To manage data, evaluate threats, and mediate rights and privileges, the Cybersurveillance State will increasingly rely upon the aggregation of data-driven systems for population management through tools such as bulk metadata collection and mass data tracking; digitized identity management programs; algorithm-driven risk-based assessments; and digital watchlisting and database screening, such as the Terrorist Watchlist and No Fly List. Consequently, biometric data will be privileged as a superior data point as the Cybersurveillance State relies on transparency of identity and identity management policy rationales. Biometric identification technologies, when combined with other biographic data collection and data fusion, facilitate the construction of digital avatars that ultimately merge the digital and physical selves. This process permits targeting potential criminal and terrorist suspects' data deemed suspect.

In a big data world, under the Cybersurveillance State, analyses of population-wide digital data—algorithmic analysis of bulk metadata, tracking of an absence of digital data, monitoring of web activity and social media presence, or behaviors linked to technological surrogates such as a smartphone—may be sufficient indicia of suspicion and guilt. Because of its breadth and rapid growth of data collection practices, and the precrime inferences from database screening and other data analytic protocols, the Cybersurveillance State poses harms that are unanticipated by our current legal system. Therefore, potential constitutional violations stemming from bureaucratized biometric cybersurveillance systems will be increasingly difficult to see and to challenge.

DISCLOSURE STATEMENT

The author is not aware of any affiliations, memberships, funding, or financial holdings that might be perceived as affecting the objectivity of this review.

LITERATURE CITED

Ahmed N. 2014. Pentagon preparing for mass civil breakdown. *Guardian*, June 12. **https://www.theguardian.com/environment/earth-insight/2014/jun/12/pentagon-mass-civil-breakdown**

Andrejevic M. 2014. Surveillance in the big data era. In *Emerging Pervasive Information and Communication Technologies (PICT): Ethical Challenges, Opportunities, and Safeguards*, ed. K Pimple, pp. 55–69. Law Gov. Technol. Ser. Dordrecht, Neth.: Springer

Apple Inc. 2016. *Use Touch ID on iPhone and iPad*. Cupertino, CA: Apple Inc. **https://support.apple.com/en-us/HT201371**

Assoc. Press. 2017. Companies start implanting microchips into workers' bodies. *Los Angeles Times*, Apr. 3. **http://www.latimes.com/business/technology/la-fi-tn-microchip-employees-20170403-story.html**

Balkin J. 2008. The constitution in the National Surveillance State. *Minn. Law Rev.* 93:1–25

Balkin J, Levinson S. 2006. The processes of constitutional change: from partisan entrenchment to the National Surveillance State. *Fordham Law Rev*. 75:489–535

BBC News. 2012. Black Hat: Iris scanners "can be tricked" by hackers. *BBC News*, July 26. **http://www.bbc.com/news/technology-18997580**

Bennett C, Lyon D, eds. 2008. *Playing the Identity Card: Surveillance, Security and Identification in Global Perspective*. Abingdon, UK: Routledge

boyd d, Crawford K. 2012. Critical questions for big data: provocations for a cultural, technological, and scholarly phenomenon. *Inf. Commun. Soc.* 15:662–79

Cao K, Jain A. 2016. *Hacking mobile phones using 2D printed fingerprints*. Tech. Rep. MSU-CSE-16-2, Mich. State Univ., East Lansing, MI. **http://biometrics.cse.msu.edu/Publications/Fingerprint/CaoJain_HackingMobilePhonesUsing2DPrintedFingerprint_MSU-CSE-16-2.pdf**

Citron D, Pasquale F. 2014. The scored society: due process for automated predictions. *Wash. Law Rev.* 89:1–33

Clarke R. 1988. Information technology and dataveillance. *Commun. ACM* 31(5):498–512

Cohen J. 2015. The biopolitical public domain: the legal construction of the surveillance economy. *Philos. Technol.* In press. doi:10.1007/s13347-017-0258-2

Cyber Sec. Res. Dev. 2016. *Identity Management and Data Privacy Technologies Project*. Dep. Homel. Secur. (on file with author)

Dep. Homel. Secur. 2008. *Privacy Impact Assessment for the Future Attribute Screening Technology (FAST) Project*. Washington, DC: Dep. Homel. Secur. **http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast.pdf**

Donohue L. 2012. Technological leap, statutory gap, and constitutional abyss: Remote biometric identification comes of age. *Minn. Law Rev.* 97:407–559

Duster T. 2003. *Backdoor to Eugenics*. Abingdon, UK: Routledge. 2nd ed.

Faraone C, Lipp K, Riley J. 2014. Boston trolling (part I). *digboston*, Oct. 9. **https://digboston.com/boston-trolling-part-i/**

Ferguson A. 2015. Big data and reasonable suspicion. *Univ. Pa. Law Rev.* 163:327–410

Ferguson A. 2016. The Internet of Things and the Fourth Amendment of effects. *Calif. Law Rev.* 104:805–80

Fox-Brewster T. 2015. Hacking Putin's eyes: how to bypass biometrics the cheap and dirty way with Google Images. *Forbes*, March 5. **http://www.forbes.com/sites/thomasbrewster/2015/03/05/clone-putins-eyes-using-google-images/#61c5deb54f85**

Friedland S. 2015. I spy: the new self-cybersurveillance and the "Internet of Things." *Wash. Lee Law Rev.* 72:1459–501

Furnas A. 2012. Homeland Security's "pre-crime" screening will never work. *Atlantic*, April 17. **http://www.theatlantic.com/technology/archive/2012/04/homeland-securitys-pre-crime-screening-will-never-work/255971/**

Garfinkel S. 2000. *Database Nation: The Death of Privacy in the 21st Century*. Sebastopol, CA: O'Reilly Media

Garvie C, Bedoya A, Frankle J. 2016. *The Perpetual Line-Up: Unregulated Police Face Recognition in America*. Washington, DC: Georgetown Law Cent. Priv. Technol. **http://www.perpetuallineup.org**

Gates KA. 2011. *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York: N.Y. Univ. Press

Gellman B, Soltani A. 2013. NSA tracking cellphone locations worldwide, Snowden documents show. *Washington Post*, Dec. 4. **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?utm_term = .ad43a46a2530**

Gomez A. 2013. Immigrant tracking may impede bill: Partisan split developing over biometric data on foreigners leaving U.S. *USA Today*, May 9, p. A5

Granick JS. 2017. *American Spies: Modern Surveillance, Why You Should Care, and What to Do About It*. Cambridge, UK: Cambridge Univ. Press

Greenwald G. 2014a. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Metropolitan Books

Greenwald G. 2014b. *Documents from No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. GlennGreenwald.net. **http://glenngreenwald.net/pdf/NoPlaceToHide-Documents-Compressed.pdf**

Harper J. 2006. *Identity Crisis: How Identification Is Overused and Misunderstood*. Washington, DC: Cato Inst.

Harris S. 2012. Giving in to the surveillance state. *New York Times*, Aug. 22. **http://www.nytimes.com/2012/08/23/opinion/whos-watching-the-nsa-watchers.html**

Hern A. 2014. Hacker fakes German Minister's fingerprints using photos of her hands. *Guardian*, Dec. 30. **https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands**

Horgan J. 2013. U.S. never really ended creepy "Total Information Awareness" program. *Scientific American Blog*, June 7. **http://blogs.scientificamerican.com/cross-check/2013/06/07/u-s-never-really-ended-creepy-total-information-awareness-program/**

Hu M. 2013. Biometric ID cybersurveillance. *Ind. Law J.* 88:1475–558

Hu M. 2015a. Big data blacklisting. *Fla. Law Rev.* 67:1735–809

Hu M. 2015b. Taxonomy of the Snowden disclosures. *Wash. Lee Law Rev.* 72:1679–767

Hu M. 2015c. Small data surveillance v. big data cybersurveillance. *Pepperdine Law Rev*. 42:773–844

Hu M. 2017a. Biometric surveillance and big data governance. In *The Cambridge Handbook of Surveillance Law*, ed. D Gray, S Henderson, Cambridge, UK: Cambridge Univ. Press. In press

Hu M. 2017b. Biometric cyberintelligence and the Posse Comitatus Act. *Emory Law J.* 66:697–763

Ingram M. 2013. Even the CIA is struggling to deal with the volume of real-time social data. *Gigaom*, March 20. **https://gigaom.com/2013/03/20/even-the-cia-is-struggling-to-deal-with-the-volume-of-real-time-social-data/2/**

Jesse D. 2016. MSU professor helps police crack smartphone fingerprint lock. *Detroit Free Press*, July 31. **http://www.freep.com/story/news/local/michigan/2016/07/31/michigan-state-university-fingerprint-smartphone/87719418/**

Kahn J. 2013. *Mrs. Shipley's Ghost: The Right to Travel and Terrorist Watchlists.* Ann Arbor: Univ. Mich. Press

Kalhan A. 2014. Immigration surveillance. *Md. Law Rev.* 74:1–78

Kaye D. 2013. A Fourth Amendment theory for arrestee DNA and other biometric databases. *Univ. Pa. J. Const. Law* 15:1095–160

Koerner B. 2015. Your relative's DNA could turn you into a suspect. *Wired*, Oct. 13. **https://www.wired.com/2015/10/familial-dna-evidence-turns-innocent-people-into-crime-suspects/**

Lessig L. 2006. *Code Version 2.0*. New York: Basic Books

Li SZ, Jain AK, eds. 2009. *Encyclopedia of Biometrics*. New York: Springer

Lynch J. 2012. *From fingerprints to DNA: biometric data collection in U.S. immigrant communities and beyond.* Spec. Rep., Immigr. Policy Cent., Washington, DC

Lyon D. 2007. *Surveillance Studies*. Cambridge, UK: Polity

Lyon D. 2009. *Identifying Citizens: ID Cards as Surveillance*. Hoboken, NJ: Wiley

Magnet S. 2011. *When Biometrics Fail: Gender, Race, and the Technology of Identity*. Durham, NC: Duke Univ. Press

Mayer-Schönberger V, Cukier K. 2013. *Big Data: A Revolution that Will Transform How We Live, Work, and Think*. London: John Murray

Miller G. 2012. Plan for hunting terrorists signals U.S. intends to keep adding names to kill lists. *Washington Post*, Oct. 23. **https://www.washingtonpost.com/world/national-security/plan-for-hunting-terrorists-signals-us-intends-to-keep-adding-names-to-kill-lists/2012/10/23/4789b2ae-18b3-11e2-a55c-39408fbe6a4b_story.html?utm_term=.a9e6e574ee44**

Miller G, Tate J, Gellman B. 2013. Documents reveal NSA's extensive involvement in targeted killing program. *Washington Post*, Oct. 16. **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?utm_term=.68110073e8e6**

Mnookin J. 2010. The courts, the NAS, and the future of forensic science. *Brooklyn Law Rev*. 75:1209–75

Modus Operandi. 2012. *Modus Operandi awarded $1 million U.S. Army contract for enemy and criminal behavioral recognition system.* Press Release, Dec. 12. **http://www.modusoperandi.com/modus-operandi-awarded-1-million-u-s-army-contract-for-enemy-and-criminal-behavioral-recognition-system/**

Murgia M. 2016. Biometrics will replace passwords, but it's a bad idea. *Telegraph*, May 27. **http://www.telegraph.co.uk/technology/2016/05/26/biometrics-will-replace-passwords-but-its-a-bad-idea/**

Murphy E. 2013. License, registration, cheek swab: DNA testing and the divided court. *Harvard Law Rev.* 127:161–96

Murray N. 2010. Profiling in the age of total information awareness. *Race Class* 52(2):3–24

Newman L. 2016. Hackers trick facial-recognition logins with photos from Facebook (what else?). *Wired*, Aug. 19. **https://www.wired.com/2016/08/hackers-trick-facial-recognition-logins-photos-facebook-thanks-zuck/**

Niinuma K, Unsang P, Jain A. 2010. Soft biometric traits for continuous use authentication. *IEEE Trans. Inf. Forensics Secur.* 5(4):771–80

O'Harrow R. 2005. *No Place to Hide*. New York: Free

O'Neill C. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown

Pasquale F. 2016. *The Black Box Society: The Secret Algorithms that Control Money and Information*. Cambridge, MA: Harvard Univ. Press

Pato J, Millett L, eds. 2010. *Biometric Recognition: Challenges and Opportunities*. Washington, DC: Natl. Acad. Press

Poindexter J. 2002. *Overview of the Information Awareness Office*. Presented at DARPATech 2002 Conf., Anaheim, CA, Aug. 2. **http://fas.org/irp/agency/dod/poindexter.html**

Poitras L, Rosenbach M, Sontheimer M, Stark H. 2014. How the NSA helped Turkey kill Kurdish rebels. *Intercept*, Aug. 31. **https://theintercept.com/2014/08/31/nsaturkeyspiegel/**

Pres. Counc. Advis. Sci. Technol., Exec. Off. Pres. (PCAST). 2014. *Big data and privacy: a technological perspective*. Rep. Pres., Washington, DC

Public Intelligence. 2014. Identity dominance: the U.S. military's biometric war in Afghanistan. *Public Intelligence*, Apr. 21. **https://publicintelligence.net/identity-dominance/**

Ramos N. 2014. City used high-tech tracking software at '13 Boston Calling. *Boston Globe*, Sept. 8. **https://www.bostonglobe.com/metro/2014/09/07/boston-watching-city-acknowledges-surveillance-tests-during-festivals/Sz9QVurQ5VnA4a6Btds8xH/story.html**

Richards N. 2013. The dangers of surveillance. *Harvard Law Rev.* 126:1935–65

Richards N, King J. 2013. Three paradoxes of big data. *Stanf. Law Rev.* 66:41–46

Ries L. 2010. B-Verify: transforming E-Verify into a biometric employment verification system. *Albany Gov. Law Rev.* 3:271–321

Risen J, Poitras L. 2014. N.S.A. collecting millions of faces from web images. *New York Times*, May 31. **http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html**

Rosen J. 2005. *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age*. New York: Random House

Roth A. 2010. Safety in numbers: deciding when DNA alone is enough to convict. *NYU Law Rev.* 85:1130–85

Scahill J, Devereaux R. 2014. Blacklisted: the secret government rulebook for labeling you a terrorist. *Intercept*, July 23. **https://theintercept.com/2014/07/23/blacklisted/**

Scahill J, Greenwald G. 2014. The NSA's secret role in the U.S. assassination program. *Intercept*, Feb. 9. **https://firstlook.org/theintercept/article/2014/02/10/the-nsas-secret-role/**

Schneier B. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W.W. Norton

Schneier B. 2016. Apple patents collecting biometric information based on unauthorized device use. *Schneier on Security Blog*, Aug. 29. **https://www.schneier.com/blog/archives/2016/08/apple_patents_c.html**

Schumer C, Graham L. 2010. The right way to mend immigration. *Washington Post*, March 19. **http://www.washingtonpost.com/wp-dyn/content/article/2010/03/17/AR2010031703115.html?utm_term=.8f9a895a857b**

Shachtman N. 2011. Army tracking plan: drones that never forget a face. *Wired*, Sept. 28. **http://www.wired.com/dangerroom/2011/09/drones-never-forget-a-face/**

Shachtman N. 2012. Air Force's top brain wants a "social radar" to "see into hearts and minds." *Wired.com*, Jan. 19. **http://www.wired.com/2012/01/social-radar-sees-minds/**

Shane P. 2007. The bureaucratic due process of government watch lists. *George Wash. Law Rev.* 75:804–55

Shockley B. 2014. Vigilant solutions unveils mobile companion app at IACP. *Vigilant Solutions*, Oct. 23. **https://vigilantsolutions.com/stories-from-the-street/vigilant-mobile-companion-app-iacp**

Slobogin C. 2008. Government data mining and the Fourth Amendment. *Univ. Chic. Law Rev*. 75:317–41

Slobogin C. 2014. Panvasive surveillance, political process theory, and the nondelegation doctrine. *Georgetown Law J*. 102:1721–76

Sobel R. 2002. The demeaning of identity and personhood in national identification systems. *Harvard J. Law Technol.* 15:319–87

Solove D. 2002. Digital dossiers and the dissipation of Fourth Amendment privacy. *South. Calif. Law Rev.* 75:1083–168

Spiro P. 2014. Expatriating terrorists. *Fordham Law Rev*. 82:2169–87

Steinbock D. 2006. Designating the dangerous: from blacklists to watch lists. *Seattle Univ. Law Rev*. 30:65–118

Strahilevitz L. 2012. Signaling exhaustion and perfect exclusion. *J. Telecommun. High Technol. Law* 10:321–30

Strandburg KJ, Raicu DS, eds. 2006. *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*. New York: Springer

Tau B. 2015. No-fly list is only one of many U.S. watchlists. *The Wall Street Journal*, Dec. 8. **http://www.wsj.com/articles/no-fly-list-is-only-one-of-many-u-s-watchlists-1449570602**

Thomson L. 2007. Critical issues in identity management—challenges for homeland security. *Jurimetr. J.* 47:335–56

TruthMove. 2016. *Total Information Awareness (TIA) System*. TruthMove. **http://www.truthmove.org/workspace/photos-content/tia_screenshot.gif**

US Dep. Def. 2011. *Terms & definitions of interest for DoD counterintelligence professionals*. Glossary (unclassified), Off. Counterintell., Def. CI & HUMINT Cent., Def. Intell. Agency, May 2. **http://fas.org/irp/eprint/ci-glossary.pdf**

US Gen. Account. Off. 2002. *Technology assessment: using biometrics for border security*. Rep. GAO-03–174, US Gen. Account. Off., Washington, DC. **http://www.gao.gov/assets/160/157313.pdf**

US Gov. Account. Off. 2010. *Employment verification: Federal agencies have taken steps to E-Verify, but significant challenges remain*. GAO-11–146, US Gen. Account. Off., Washington, DC. **http://www.gao.gov/assets/320/314278.pdf**

USA Today. 2003. Pentagon's "Terror Information Awareness" program will end. *USA Today*, Sept. 25. **http://usatoday30.usatoday.com/news/washington/2003-09-25-pentagon-office_x.htm**

Vacca J. 2007. *Biometric Technologies and Verification Systems*. Burlington, MA: Butterworth-Heinemann

Wittes B, Blum G. 2015. *The Future of Violence: Robots and Germs, Hackers and Drones*. New York: Basic Books

Yakowicz W. 2016. How collecting biometric information from employees and customers could get you sued. *Inc*., May 12. **http://www.inc.com/will-yakowicz/legal-risks-of-biometrics-at-the-office.html**

Zuboff S. 2015. Big other: surveillance capitalism and the prospects of an information civilization. *J. Inf. Technol.* 30:75–89

Annual Review of Law and Social Science

Volume 13, 2017

Contents