Article

Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age

Laura K. Donohue[†]

† Associate Professor of Law, Georgetown Law. Special thanks to Mary Bullard, June E. Kuhn, and Todd Venie for their research assistance. Stuart Baker, David Ball, Julie Cohen, Carrie Cordero, Jennifer Grannick, Aziz Huq, Greg Klass, Harvey Rishikof, Mike Seidman, Babak Siavoshy, and Abbe Smith provided thoughtful comments on the text. The Article further benefited from suggestions made at the Georgetown Law Faculty Workshop; the Electronic Privacy Information Center's Privacy Coalition; the George Washington Law School-Berkeley Law—Privacy Law Scholars Conference; and the University of Virginia Law National Security Law Institute. Thanks to the staff and editors of the *Minnesota Law Review* for their assistance and attention to detail. Thanks also to Kate Zerwas Graham, and Brennan Furness, for their assistance with Bluebooking and edits.

INTRODUCTION

On January 23, 2012, the Supreme Court ruled that the installation and use of a Global Positioning System (GPS) device constitutes a search within the meaning of the Fourth Amendment.[1] What might appear to be a victory for privacy advocates, however, was rooted in a concept of law that is obsolete in the face of new and emerging tracking technologies.

In *United States v. Jones*, the government obtained a warrant granting law enforcement officers ten days to install a GPS tracking device in a car owned by the wife of a suspected

1. United States v. Jones, 132 S. Ct. 945, 949 (2012).

drug dealer.[2] On the eleventh day, agents actually installed the device—not in Washington, D.C., as required by the warrant, but in Maryland.[3] For the next twenty-eight days, the Government tracked the vehicle, later using the information to indict the car owner's husband, Antoine Jones, on drug trafficking conspiracy charges.[4] Four members of the Court joined Justice Antonin Scalia in relying not on whether agents had violated Jones's reasonable expectation of privacy—the test commonly applied to the use of electronic surveillance—but on the ancient common law of trespass.[5]

Justice Scalia explained, "It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information."[6] Such an intrusion "would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."[7]

True. But the Bill of Rights came into effect on December 15, 1791. Two hundred and twenty years later, focusing on the physical placement of the GPS device ignores the growing body of tracking technologies that make no contact with the individual. Remote identification is the law enforcement tool of the future. GPS is only an interim step.

Consider facial recognition technology (FRT). Complex algorithms measure the size, angle, and distance between features, enabling identification based on facial characteristics.[8] Paired with video, this technology allows governments to observe and record actions in public space and to recall this information for any number of reasons. Such remote tracking is not the equivalent of placing a tail on a suspect. It requires no suspicion of any individual; it functions as warrantless mass surveillance. It is inexpensive. It has perfect recall. And it generates terabytes of new knowledge. As the court below noted in *United States v. Maynard*,

2. *Id.* at 948–49.

3. *Id.* at 948.

4. *Id.*

5. *See id.* The five justices did not address whether the search was reasonable within the meaning of the Fourth Amendment. Justice Sotomayor filed a concurring opinion, as did Justice Alito, who was joined by Justices Breyer, Ginsburg, and Kagan.

6. *Id.* at 946 (2012).

7. *Id.*

8. *See Face Recognition—Technology Overview*, EX-SIGHT.COM, http://www.ex-sight.com/technology.htm (last visited Oct. 28, 2012).

> A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.[9]

This level of intrusiveness suggests something different in kind, not degree, from what has come before. It is quickly becoming more common.

Patents alone demonstrate that the technology has come of age.[10] Between 1970 and 1995, the U.S. Patent Office granted fewer than 10 patents involving facial recognition.[11] From 1995 to 2000, it issued 20 such patents.[12] Between 2001 and 2011, the number leapt to 633.[13]

These patents are increasingly focused on, and applicable to, law enforcement and national security, where applications range from confirming targets for elimination and pairing photographs and data from different databases, to monitoring individuals as they move through public space. Between 1970 and 1995, none of the patents specifically focused on law enforcement or national security. Of the patents issued between 1995 and 2000, less than half were directed at such uses. But following 9/11, three major facial recognition patent clusters with direct law enforcement and national security applications emerged: digital video (80 patents), image surveillance (35) and biometric identification data (136). (See Figure 1).[14]

9. United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

10. But note the myriad problems that persist with FRT. *See, e.g.*, E-mail from C. L. Wilson, Nat'l Inst. of Standards & Tech., to Travis L. Farris, Janet M. Boodro, Roy Weise, Tom Hopper & John Atkins (Dec. 2, 2003, 08:29 EST), *available at* http://www.dhs.gov/xlibrary/assets/usvisit/US_VISIT_NIST-DHS_Coordinated_Doc.pdf (noting low probability of verification in outdoor illumination).

11. The timing and frequency of patents was ascertained by the author by conducting structured searches of restricted time intervals in a patent search engine. *See* PRIORIP, http://www.prior-ip.com (last visited Sept. 18, 2012) (website no longer available).

12. *See supra* note 11.

13. The number of FRT patents issued per year is as follows: 1995 (2); 1996 (2); 1997 (0); 1998 (7); 1999 (3); 2000 (6); 2001 (4); 2002 (12); 2003 (30); 2004 (17); 2005 (10); 2006 (57); 2007 (57); 2008 (90); 2009 (100); 2010 (167); 2011 (89). *See supra* note 11.

14. *See supra* note 11.

Figure 1
Facial Recognition Patents 1995–2011

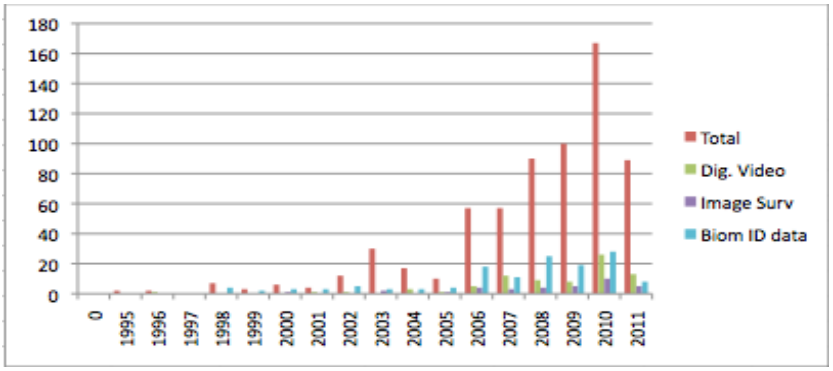


Figure 1: Total and in three key clusters: digital video, image surveillance, and biometric data.

Further examination demonstrates a growing government market in this area.[15] Major defense contractors such as Lock-

15. *See, e.g.*, Distributed Stand-off ID Verification Compatible with Multiple Face Recognition Systems, U.S. Patent No. 7,817,013 (filed Dec. 1, 2005) (issued Oct. 19, 2010) (describing the technology as "providing stand-off biometric verification of a driver of a vehicle while the vehicle is moving and/or a person on foot at a control gate" and assigned to Honeywell International Inc.); Distributed Stand-off Verification and Face Recognition Systems, U.S. Patent No. 7,843,313 (filed Dec. 1, 2005) (issued Nov. 30, 2010) (providing same capability as U.S. Patent 7,817,013, filed on same day, and also assigned to Honeywell International Inc.); Identification of an Object in Media and of Related Media Objects, U.S. Patent No. 7,787,697 (filed June 9, 2006) (issued Aug. 31, 2010) (pairing of audio and visual biometric identification in a mobile device; and assigned to Sony Ericsson Mobile Commission AB); Mobile Self-Contained Networked Checkpoint, U.S. Patent No. 7,789,258 (filed May 7, 2007) (issued Sept. 7, 2010) (providing a portable checkpoint system that allows for facial recognition and assigned to the U.S. as represented by the Secretary of the Navy); Real-Time Facial Recognition and Verification Systems, U.S. Patent No. 7,130,454 (filed Mar. 15, 2002) (issued Oct. 31, 2006) (providing a "system and method for acquiring, processing, and comparing an image with a stored image to determine if a match exists," using pre-stored color values, such as flesh tone; assigned to Viisage Technology, Inc.); Security System Control for Monitoring Vehicular Compartments, U.S. Patent No. 7,768,380 (filed Oct. 29, 2007) (issued Aug. 3, 2010) (providing a security system for monitoring vehicular compartments by scanning and using facial recognition to identify the driver and passengers; assigned to Automotive Technologies International, Inc). A similar picture emerges when looking at the specific companies involved. VideoIQ, Inc., for example, obtained a patent for local verification systems and security monitoring technologies. U.S. Patent No. 7,504,942 (filed Feb. 6, 2006) (issued Mar. 17, 2009). The company's customers range from

heed Martin and Honeywell International, together with myriad startups dedicated to FRT and video technologies, have swiftly moved into related technologies. Simultaneously, government agencies, such as the Central Intelligence Agency (CIA), the Defense Advanced Research Projects Agency, the Air Force Research Laboratory (DARPA), and the National Geospatial-Intelligence Agency, have invested in advanced technologies that range from behavior recognition, motion pattern learning, and anomaly detection, to object recognition and tracking.[16]

Government forays into biometric identification abound. The Federal Bureau of Investigation (FBI), for example, is currently developing what it calls Next Generation Identification (NGI).[17] One of its components, the Interstate Photo System,

commercial and educational interests to municipalities, transportation and government, including the Department of Homeland Security. *Customers*, VIDEOIQ, http://www.videoiq.com/customers.php (last visited Nov. 2, 2012).

16. *See, e.g.*, *Biography of Anthony Hoogs: Senior Director of Computer Vision*, KITWARE, http://www.kitware.com/company/team/hoogs.html (last visited Nov. 2, 2012) (listing Dr. Hoogs as the principal investigator in various DARPA projects). Dr. Hoogs has researched extensively in the field of biometric identification. *See, e.g.*, Kobus Barnard et al., *Evaluation of Localized Semantics: Data, Methodology, and Experiments*, 77 INT'L J. COMPUTER VISION 199, 216 (2008) (acknowledging financial support from Lockheed Martin); Zhaohui Sun & Anthony Hoogs, *Image Comparison by Compound Disjoint Information with Applications to Perceptual Visual Quality Assessment, Image Registration and Tracking*, 88 INT'L J. COMPUTER VISION 461, 461 (2010) (listing GE Global research as Dr. Hoogs's institutional affiliation); Michael T. Chan et al., *Event Recognition with Fragmented Object Tracks*, 18 INT'L CONF. PATTERN RECOGNITION (2006) (noting support from Lockheed Martin); Michael T. Chan et al., *Joint Recognition of Complex Events and Track Matching* 2006 IEEE COMPUTER SOC. CONF. COMPUTER VISION PATTERN RECOGNITION PROC. 1615, 1615–22 (2006) (same); Naresh P. Cuntoor et al., *Track Initialization in Low Frame Rate and Low Resolution Videos*, 20 INT'L CONF. PATTERN RECOGNITION PROC. 3640, 3640–44 (2010); Anthony Hoogs et al., *Detecting Semantic Group Activities Using Relational Clustering*, 2008 IEEE WORKSHOP MOTION VIDEO COMPUTING PROC. 1, 1–8 (sponsored by Lockheed Martin), *available at* http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4544062; Anthony Hoogs & Roderic Collins, *Object Boundary Detection in Images Using a Semantic Ontology*, 2006 CONF. COMPUTER VISION PATTERN RECOGNITION WORKSHOP PROC., *available at* http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=arnumber=164054; Anthony Hoogs & A.G. Amitha Perera, *Video Activity Recognition in the Real World (National Conference on Artificial Intelligence)* 23 AAAI CONF. ARTIFICIAL INTELLIGENCE PROC. 1551, 1551 (2008) (noting applications for technology in observing "stealing, fighting, exchanging, packages, and covert surveillance"), *available at* http://www.aaaipress.org/Papers/AAAI/2008/AAAI08-260.pdf.

17. *See Fingerprints & Other Biometrics: Next Generation Identification*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi (last visited Nov. 2, 2012).

allows law enforcement to submit still images or video surveillance feeds obtained from any public or private source.[18] The system is designed to store this data and, using FRT, to identify individuals, pairing images with biographic information.[19] NGI also uses biographic information to search its Repository for Individuals of Special Concern (RISC).[20] This database consists of records of "known or appropriately suspected terrorists," as well as "other persons of special interest" (a category that remains undefined).[21] NGI further includes a Rap Back Service, where employers can collect employees' biometric data and give it to the FBI, which will then notify them of any criminal, and, in some cases, civil activities.[22] This means that everything from criminal convictions to parking tickets to attendance at political rallies, captured on film, could be reported.

The FBI is not alone. In 2004, the Department of Defense's (DoD) Automated Biometric Identification System (ABIS), designed to work with the FBI's biometric database, became op-

18. *See Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS)*, FED. BUREAU OF INVESTIGATION (2008), http://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system [hereinafter *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS)*], (stating that photos may be obtained from security cameras, friends, and family). *But see What Facial Recognition Technology Means for Privacy and Civil Liberties: Hearing Before the Sub comm. on Privacy, Tech. & the Law of the S. Judiciary Comm.*, 105th Cong. 3 (2012) (statement of Jerome M. Pender, Deputy Dir. Crim. Just. Info. Servs. Div., FBI), *available at* http://www.judiciary.senate.gov/pdf/12-7-18PenderTestimony.pdf ("Only criminal mug shots are used to populate the national repository.").

19. *See Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS)*, *supra* note 18.

20. *What Facial Recognition Technology Means for Privacy and Civil Liberties*, *supra* note 18, at 2.

21. *Fingerprints & Other Biometrics: Repository for Individuals of Special Concern (RISC)*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi/repository-for-individuals-of-special-concern-risc (last visited Nov. 2, 2012).

22. *See 5 Things You Should Know About the FBIs Massive New Biometric Database (Alternet)*, UNCOVER THE TRUTH (Jan. 10, 2012), http://uncoverthetruth.org/press/5-things-you-should-know-about-the-fbis-massive-new-biometric-database-alternet; *see also* FED. BUREAU OF INVESTIGATION, ELECTRONIC BIOMETRIC TRANSMISSION SPECIFICATION (EBTS) 60 (2007), *available at* https://www.fbibiospecs.org/docs/EBTSv8.0_20070924.pdf (noting that the service will allow authorized agencies to enroll and receive notifications about individual criminal activity and possibly civil activity if not legally prohibited).

erational.[23] By 2009, DoD's database had evolved into the Next Generation ABIS, a system that combines fingerprint, palm print, facial recognition, and iris analysis with biographic and encounter transactions.[24] It stores, retrieves, and searches data collected from "persons of national security interest."[25] DoD has complemented this initiative with a Biometrically-Enabled Watchlist.[26] The Department of Homeland Security (DHS) and the State Department also maintain biometric databases and watchlists.[27] Memoranda of understanding between the agencies focus on how to make these systems interoperable.[28]

Despite the explosion of federal initiatives in this area, Congress has been virtually silent on the many current and potential uses of FRT and related technologies.[29] No laws directly address facial recognition—much less the pairing of facial

23. NAT'L SCI. & TECH. COUNCIL, THE NATIONAL BIOMETRICS CHALLENGE 6 (2011), *available at* http://www.biometrics.gov/Documents/BiometricsChallenge2011_protected.pdf.

24. BIOMETRICS TASK FORCE, DEP'T OF DEF., ANNUAL REPORT 10 (2009), *available at* http://www.fas.org/man/eprint/biometric09.pdf.

25. BIOMETRICS TASK FORCE, DEP'T OF DEF., ELECTRONIC BIOMETRIC TRANSMISSION SPECIFICATION 1 (2009) [hereinafter BIOMETRICS TASK FORCE], *available at* http://www.biometrics.gov/standards/DoD_ABIS_EBTS_v2.0.pdf.

26. *See* BIOMETRICS IDENTITY MGMT. AGENCY, DOD BIOMETRICS COLLABORATION FORUM 14 (2011) [hereinafter DOD BIOMETRICS COLLABORATION FORUM], *available at* http://www.biometrics.dod.mil/Files/Documents/2011_Collaborations/ForumReport.pdf.

27. *See Government Agencies Using US-VISIT*, DEP'T OF HOMELAND SECURITY, http://www.dhs.gov/government-agencies-using-US-visit (last visited Nov. 2, 2012).

28. *See* NAT'L SCI. & TECH. COUNCIL, *supra* note 23, at 8.

29. *See, e.g.*, DNA Fingerprint Act of 2005, Pub. L. No. 109-162, §§ 1001–1005, 119 Stat. 2960, 3084–86 (codified as amended in scattered sections of 18 U.S.C. and 42 U.S.C.) (creating opt-out system for expunging DNA profiles from the national index and authorizing collection of DNA samples from persons arrested or detained under federal law); Justice for All Act of 2004, Pub. L. No. 108-405, §§ 202–203 118 Stat. 2260, 2266–71 (codified as enacted in scattered sections of 18 U.S.C., codified as amended in scattered sections of 10 U.S.C. and 42 U.S.C., and codified as repealed in 42 U.S.C. § 10606) (enhancing provisions for DNA collection and analysis, and providing for post-conviction DNA testing). But note that in October 2011, Senator John D. Rockefeller IV (D-W. Va.), requested that the Federal Trade Commission consider the privacy impact of FRT with a report due February 9, 2012. Brian Heaton, *Facial Recognition Technology Spurs Privacy Concerns for Feds*, GOV'T TECH. (Oct. 21, 2011), http://www.govtech.com/public-safety/Facial-Recognition-Privacy-Concerns-Feds.html. The report largely recommends industry self-regulation as opposed to legislative action. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESS AND POLICYMAKERS i (2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

recognition with video surveillance—in either the criminal law or foreign intelligence realm. Many of the existing limits placed on the collection of personally identifiable information do not apply. Only a handful of hearings has even questioned the use of biometrics in the national security or law enforcement context.[30]

The absence of a statutory framework is a cause for significant concern. Facial recognition represents the first of a series of next generation biometrics, such as hand geometry, iris, vascular patterns, hormones, and gait, which, when paired with surveillance of public space, give rise to unique and novel questions of law and policy.[31] These constitute what can be considered Remote Biometric Identification (RBI). That is, they give the government the ability to ascertain the identity (1) of multiple people; (2) at a distance; (3) in public space; (4) absent notice and consent; and (5) in a continuous and on-going manner. As such, RBI technologies present capabilities significantly different from that which the government has held at any point in U.S. history.

Hitherto, identification techniques centered on what might be called Immediate Biometric Identification (IBI)—or the use of biometrics to determine identity at the point of arrest, following conviction, or in conjunction with access to secure facilities. Fingerprint is the most obvious example of IBI, although more recent forays into palm prints fall within this class. DNA technologies that require individuals to provide saliva, skin, or other samples for analysis also can be considered as part of IBI. Use of technology for IBI, in contrast to RBI, tends to be focused (1) on a single individual; (2) close-up; (3) in relation either to custodial detention or in the context of a specific physical area related to government activity; (4) in a manner often

30. For a notable exception, see *Hearing on Oversight of the Federal Bureau of Investigation Before the S. Judiciary Comm.*, 110th Cong. 92 (2008) (statement of Sen. Patrick Leahy, Chairman, S. Comm. on the Judiciary) ("Recent reports suggest that the FBI is engaged in a $1 billion program to create a massive biometric database, compiling not just fingerprints, but eye scans, palm prints, facial features, and other identifying features of millions of people. It is vitally important for the FBI to master emerging and enhanced technologies in the fight against crime and terrorism. But we must also be cognizant of the impact that such a database can have on the privacy rights and civil liberties of Americans.").

31. *See* NAT'L SCI. & TECH. COUNCIL, BIOMETRICS "FOUNDATION DOCUMENTS," 4–6, http://www.biometrics.gov/documents/biofoundationdocs.pdf (last visited Nov. 2, 2012) (providing an overview of current and emerging biometric technology).

involving notice and often consent;[32] and (5) is a one-time or limited occurrence. The types of legal and policy questions raised by RBI differ from those accompanying IBI.

What we are witnessing, as a result of the expansion from IBI to RBI, is a sea change in how we think about individuals in public space. Congress has yet to grapple with the consequences.

This Article seeks to drive the discussion forward by detailing the recent explosion of federal initiatives in biometric identification, highlighting gaps in the current statutory framework governing RBI, and considering the Court's jurisprudence in relation to the constitutional questions that arise. Arguing that the current statutory and constitutional framing is inadequate to address the new conditions that accompany these emerging technologies, it calls for immediate and careful congressional consideration of RBI.

Part I begins with a discussion of the evolution of biometric technologies and federal programs. Prior to September 11, 2001, there were relatively few initiatives focused on the collection and use of biometrics. Immediately following the attacks, resources flowed to this area. Initially, most of the attention centered on U.S. borders. Over the next decade, the patterns shifted. Paralleling the evolution of applications related to homeland security came efforts to expand biometrics to government employees. Traditional law enforcement collection of fingerprints expanded to include other forms of biometric data. Similar systems worked their way into the military infrastructure, with soldiers using new tools for targeting, identification, and surveillance purposes. New technologies began to extend horizontally, across federal agencies, as well as vertically, to state and local governments. Emphasis is now moving beyond merely establishing biometric systems to facilitating information sharing between these databases, blurring the line between investigations and intelligence gathering.

Part II considers the statutory frameworks that potentially apply to the current systems: government acquisition of individually identifiable data, criminal warrant requirements, and foreign intelligence surveillance. In relation to the first, federal

32. An important exception here would be the lifting of prints or collection of DNA from a crime scene, where neither consent nor notice would be present; such a scenario, however, is contemplated in the context of (2)—i.e., a limited geographic area related to government activity, in this case the investigation of a crime.

agencies have considerable, largely unchallenged authority to collect and analyze personally identifiable information. Congressional restrictions on the exercise of such authorities generally do not apply to biometric systems. Gaps in the 1974 Privacy Act and its amendments and the 1990 Computer Matching and Privacy Protection Amendments, in conjunction with Privacy Act exemptions and the 2002 E-Government Act, minimize the extent to which such instruments can be brought to bear. The second area turns on Title III of the 1968 Omnibus Crime Control and Safe Streets Act and Title I of the 1986 Electronic Communications Privacy Act. Neither statute, however, directly addresses RBI. The third area, controlled by the 1978 Foreign Intelligence Surveillance Act (FISA) and its amendments, similarly falls short. It is unclear whether biometric surveillance is considered as within the Foreign Intelligence Court's remit. Even if it is, significant questions exist as to whether FISA's provisions can be met by RBI. In the absence of a statutory framework with which to evaluate the current federal initiatives and their potential inclusion of facial recognition and video technologies, we are driven back upon constitutional considerations.

Part III recognizes that RBI sits uneasily in the Court's Fourth Amendment jurisprudence, which has yet to squarely address the implications of these new technologies. Potentially applicable lines of cases depend upon conditions that fail to provide meaningful distinctions within RBI.

Part IV notes that little relief may be found in associated constitutional doctrines. The Fifth Amendment's right against self-incrimination, understood as protecting individuals from being forced to take action, fails to reach the passive nature of ubiquitous surveillance. The First Amendment's protection of speech and assembly present a low bar, even where RBI may be directly targeting political rallies. The Fifth and Fourteenth Amendments' due process protections key in on the accuracy of the technology—something that may become less of an issue as research advances.

Part V concludes with the recognition that the types of questions posed by this technology may require a new approach to the place of privacy in society. Instead of focusing on the rights discourse as a framing for personally identifiable information, it may be more important to think about privacy in a constitutive sense—i.e., as playing a role in social cohesion and personal and social development. Simultaneously, ways of iden-

tifying the technologies thus implicated, and of understanding their impact, need to be developed—this, in juxtaposition to the unmitigated embrace of new and emerging technologies and the assumption that such advances represent something merely different in degree, not kind, from what has come before.

I. TECHNOLOGICAL LEAP

For more than a century, U.S. law enforcement agencies have employed biometric identification.[33] Such technologies initially took the form of fingerprinting. In the early twentieth century, the New York Police Department, the New York State Prison System, and the Federal Bureau of Prisons became the first to adopt this technique.[34] Soon thereafter, the U.S. Army found a parallel use in the national security realm.[35] In 1907, fingerprinting spread to the U.S. Navy and the following year to the U.S. Marine Corps (USMC).[36] The use of fingerprints proved labor intensive, requiring numerous people and hours to

33. In 1892, Sir Francis Galton published his famous treatise, *Finger Prints*, establishing their individuality and permanence and offering the first classification system to distinguish between persons. Laura A. Hutchins, *Systems of Friction Ridge Classification*, *in* THE FINGERPRINT SOURCEBOOK 5-1, 5-6 (Alan McRoberts ed., 2011), *available at* https://www.ncjrs.gov/pdffiles1/nij/225325.pdf. Edward Richard Henry followed Galton's work with his *Classification and Uses of Finger Prints*, providing a more easily searchable system with straightforward methods of classification and comparison. EDWARD RICHARD HENRY, CLASSIFICATION AND USES OF FINGER PRINTS 3–14 (1905) (discussing Galton's work and noting the degree to which fingerprinting had become integrated into military and civil functions in India). These studies, together with growing interest in the topic, prompted the British Home Office to conduct an inquiry into the identification of criminals by measurement and fingerprints. *History of the Metropolitan Police*, METROPOLITAN POLICE, http://www.met.police.uk/history/fingerprints.htm (last visited Nov. 2, 2012). By 1901 New Scotland Yard had launched its first Fingerprint Branch, adopting Henry's system of classification. *Id.*

34. *Fingerprints: The First ID*, FINDLAW, http://criminal.findlaw.com/crimes/more-criminal-topics/evidence-witnesses/fingerprints-the-first-id.html (last visited Nov. 2, 2012) (noting that Scotland Yard used fingerprinting in 1901 before American agencies began using it in 1903).

35. *See id.*

36. Jeffery G. Barnes, *History*, *in* THE FINGERPRINT SOURCEBOOK 1-1, 1-19 (Alan McRoberts ed., 2011), *available at* https://www.ncjrs.gov/pdffiles1/nij/225320.pdf; *see The History of Fingerprints*, ONIN.COM, http://onin.com/fp/fphistory.html (last visited Nov. 2, 2012). By 1928 the FBI had similarly begun using fingerprint identification. *Aviation Security: Challenges in Using Biometric Technologies*: *Testimony Before the Subcomm. on Aviation of the H. Comm. on Transp. & Infrastructure*, 108th Cong. 17 (2004) (statement of Keith A. Rhodes, Chief Technologist, Applied Research & Methods), *available at* http://www.gao.gov/new.items/d04785t.pdf.

identify, catalogue, and compare prints stored on paper.[37] Starting in the 1960s, the introduction of automated technology for comparison and storage altered the landscape—complex analyses could be completed within seconds.[38] Digitization further sped the number of records that could be stored and analyzed.

By the end of the twentieth century, automated fingerprint matching had become the norm and new forms of biometric identification had begun to emerge.[39] The government launched a number of initiatives aimed at taking advantage of the new technologies. The National Institute of Standards and Technology and the Biometric Consortium (established in 1992) created an interagency body to consider and coordinate biometric activities at the federal level.[40] Most of the programs underway emphasized fingerprint and DNA as methods of identification, with further interest in facial recognition and iris analysis.[41] Accordingly, the FBI established its Integrated Automated Fingerprint Identification System (IAFIS), while the Immigration and Naturalization Service (INS) initiated an automated biometric identification system called IDENT.[42] The FBI also created the Combined DNA Index System, known as CODIS, a computer database that integrates local, state, and federal DNA records of convicted offenders, evidence collected from crime scenes, and missing persons.[43]

37. PETER KOMARINSKI, AUTOMATED FINGERPRINT IDENTIFICATION SYSTEMS 8–10 (2005).

38. *Id.* at 10–11; NAT'L SCI. & TECH. COUNCIL, BIOMETRICS IN GOVERNMENT POST-9/11: ADVANCING SCIENCE, ENHANCING OPERATIONS 8 (2008) [hereinafter BIOMETRICS IN GOVERNMENT POST-9/11], *available at* http://www.biometrics.gov/Documents/Biometrics%20in%20Government%20Post%209-11.pdf (dating research conducted by the FBI and NIST on the automated matching of fingerprints to 1967).

39. The first patent granted for automated iris recognition, for instance, was issued in 1994. *Introduction to Iris Recognition*, UNIV. CAMBRIDGE, http://www.cl.cam.ac.uk/users/jgd1000/iris_recognition.html (last visited Nov. 2, 2012).

40. BIOMETRICS IN GOVERNMENT POST-9/11, *supra* note 38, at 6.

41. *See id.* at 8. In 1993, the Immigration and Naturalization Service launched INSPASS, a system based on hand geometry, used to facilitate swifter processing of business travelers registered for the program. *Id.* In 1995, there was a commercial release of iris prototypes. *Id.* In 1996, INS launched a fully automated Port of Entry at Scobey, Montana, relying upon voice verification technology. *Id.*

42. *See id.*

43. *See Laboratory Services: Combined DNA Index System (CODIS)*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/lab/codis (last visited Nov. 2, 2012).

Following the attacks of 9/11, renewed interest in biometrics led to an expansion of the existing databases, the institution of new programs, and the creation of new inter-agency agreements to allow for the sharing of biometric data.[44] Like the civilian institutions, the military vigorously pursued new uses of biometric technologies, creating in the process its own database known as the Automated Biometric Identification System, with further expansion resulting in the creation of Next Generation ABIS.[45] Federal initiatives reached beyond horizontal coordination, to include vertical integration with state and local government.[46]

A. PRE-9/11 FEDERAL DEVELOPMENT OF BIOMETRIC TECHNOLOGY AND COLLECTION SYSTEMS

Two federal fingerprint repositories and one DNA database predated the September 11, 2001 attacks. A brief discussion of each helps to illustrate the changed circumstances that followed.

The first initiative stemmed from research jointly sponsored in 1967 by the FBI and the National Institute of Standards and Technology.[47] More than a quarter of a century later, the FBI began planning development of IAFIS, which became operational in 1999.[48] IAFIS collected ten-print images, entered by local, state, and federal law enforcement agencies.[49] It quickly came to serve as a national repository, allowing officials to check new prints against the database, and to correlate the prints to individual identity.[50]

Throughout the 1990s, talks between the FBI and INS as to whether the latter could use IAFIS for border security ex-

44. *See* BIOMETRICS IN GOVERNMENT POST-9/11, *supra* note 38, at 20, 26.

45. *See id.* at 25.

46. *See id.* at 29 (describing coordination of US-VISIT service amongst federal, state, and local agencies).

47. *See* BIOMETRICS IN GOVERNMENT POST-9/11, *supra* note 38, at 8–9. It took more than twenty years for the American National Standards Institute (ANSI) to release a national standard. AM. NAT'L STANDARDS INST., AM. NAT'L STANDARD FOR INFORMATION SYSTEMS—FINGERPRINT IDENTIFICATION—DATA FORMAT FOR INFORMATION INTERCHANGE (1986), *available at* http://biometrics.nist.gov/cs_links/standard/archived/ANSI-NIST-ICST_1-1986.pdf.

48. BIOMETRICS IN GOVERNMENT POST-9/11, *supra* note 38, at 8–9.

49. *See Integrated Automated Fingerprint Identification System*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis (last visited Nov. 2, 2012).

50. *See id.*

posed schisms in the agencies' needs.[51] INS, which was developing its own automated biometric system, emphasized the importance of being able to process a high volume of inquiries swiftly.[52] The movement of large numbers of people and limited facilities for holding individuals at points of entry made it difficult to accommodate delays.[53] With its operational mission in mind, INS considered two fingerprints sufficient for screening those entering and leaving the country.[54] The FBI, in contrast, with an eye towards criminal prosecution, emphasized the importance of obtaining ten prints.[55] The inclusion of such information, however, made searches more complex which, correspondingly, took longer.[56]

To accommodate the special needs presented by the border, in 1994, Congress approved INS's own repository, known as IDENT.[57] Two years later, Congress authorized further development of the integrated entry and exit data system.[58] This database included photographs and two index finger fingerprints, with additional information related to the individual's criminal history.[59]

Efforts to integrate IAFIS and IDENT's parallel fingerprint systems repeatedly stalled on the shoals of institutional needs and bureaucratic politics. In 1998, for instance, Congressman Alan Mollohan, the ranking member of the House Appropriations Subcommittee for Commerce, Justice, State, and the Judiciary, wrote to Attorney General Janet Reno, ask-

51. *See* U.S. Dep't of Justice, S*tatus of IDENT/IAFIS Integration: Integration of the Fingerprint System* (Dec. 7, 2001), http://www.justice.gov/oig/reports/plus/e0203/finger.htm [hereinafter *Status of IDENT/IAFIS*].

52. *See id.*

53. *See id.*

54. *See id.*

55. *See id.*

56. *See id.*

57. *Id.* Barriers to integration at the time included different operational requirements, insufficient funds for the development of IAFIS projects, and a certain stasis that accompanied the independent development of the two repositories of data. *See generally The Rafael Resendez-Ramirez Case: A Review of the INS's Actions and the Operation of Its IDENT Automated Fingerprint Identification System*, U.S. OFFICE OF THE INSPECTOR GEN. (Mar. 20, 2000), http://www.justice.gov/oig/special/0003/index.htm (noting the failure of IDENT to identify Resendez as an individual wanted by the FBI).

58. *See* Immigration and Naturalization Service Data Management Improvement Act of 2000, Pub. L. No. 106-215, § 2, 114 Stat. 337, 337–39.

59. *See Status of IDENT/IAFIS*, *supra* note 51; *see also* BIOMETRICS IN GOVERNMENT POST-9/11, *supra* note 38, at 8.

ing straight out whether the two systems were redundant.[60] The Department of Justice's (DOJ) Justice Management Division insisted that they were not, in the process issuing a report considering three options: (1) to retain IDENT in its current form, while adapting it to ensure greater integration of criminal data in the two-print mode; (2) to move IDENT to a ten-print system and to retain both in parallel; or (3) to scrap IDENT and force INS to use IAFIS's ten-print system.[61] (DOJ did not consider dismantling its own database, IAFIS, in favor of INS's IDENT.) DOJ's Justice Management Division, the FBI, Border Patrol, and INS agreed that the second option would be the best one, which would have required Congress to increase funding across the board.[62] Congress refused.[63] A high profile case in 1999 again forced the question of integrating the two systems. At issue was the capture of Rafael Resendez-Ramirez, a Mexican citizen with an extensive criminal record, wanted in connection with several railway murders.[64] In June of that year, two Border Patrol agents detained him but subsequently released him when IDENT failed to include the information that he was wanted by the FBI.[65] Resendez-Ramirez committed four more murders before he surrendered to U.S. authorities the following month.[66] Congress excoriated the Executive Branch for failing to integrate IAFIS and IDENT.[67]

Even as it developed an extensive fingerprinting system, the FBI explored ways to use DNA analysis for criminal investigations. In the late 1980s the Bureau formed a Technical Working Group on DNA Analysis Methods to look more closely at this question.[68] Sponsored by the FBI Laboratory, the working group held a series of meetings to address the scientific challenges involved in deploying DNA technologies.[69] As the research progressed, in 1994, Congress modified the Omnibus Crime Control and Safe Streets Act of 1968 by adding provi-

60. *Status of IDENT/IAFIS*, *supra* note 51.
61. *Id*.
62. *Id.*
63. *Id.*
64. *Id.*
65. *Id.*
66. *Id.*
67. *Id.*
68. *See* OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUST., THE FBI DNA LABORATORY: A REVIEW OF PROTOCOL AND PRACTICE 15 (2004), *available at* http://www.justice.gov/oig/special/0405/final.pdf.
69. *See id.*

sions regulating DNA laboratories and governing the accumulation of DNA records and samples.[70] This legislation created CODIS, a database run by the FBI to store local, state, and federal DNA profiles in searchable form.[71] Four years later, the Crime Identification Technology Act provided for more effective interstate criminal justice identification, information, communications, and forensics.[72] The legislation established grants to encourage the identification and analysis of DNA.[73] By 2000, the demand for DNA analysis had outpaced the federal government's ability to process samples, leading to the passage of the DNA Analysis Backlog Elimination Act.[74]

Outside of fingerprinting and DNA, there were some forays into facial recognition. In 1993, for example, the DoD initiated the Face Recognition Technology (FERET) program.[75] The goal was to develop automatic facial recognition systems for security, intelligence, and law enforcement purposes.[76] By 1996, the Army Research Laboratory had moved to real-time video face identification within an access control context.[77] Four years later, DoD established its first Biometrics Management Office and Biometrics Fusion Center.[78] That same year DARPA initiated

70. DNA Identification Act of 1994, Pub. L. No. 103-322, § 210301, 108 Stat. 2065, 2065–66.

71. *Id.*; *see also Laboratory Services: Combined DNA Index Systems (CODIS)*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/lab/codis (last visited Nov. 2, 2012) (providing a description of the mission and work of the CODIS Unit).

72. Crime Identification Technology Act of 1998, Pub. L. No. 105-251, § 102, 112 Stat. 1870, 1870–71.

73. *Id.*

74. DNA Analysis Backlog Elimination Act of 2000, Pub. L. No. 106-546, 114 Stat. 2726. Note that these initiatives continued post-9/11. *See, e.g.*, Justice for All Act of 2004, Pub. L. No. 108-405, §§ 203, 411, 118 Stat. 2260, 2269–71, 2278–84 (enhancing DNA collection and analysis and providing for post-conviction DNA testing); DNA Fingerprint Act of 2005, Pub. L. No. 109-162, § 1002, 119 Stat. 3084, 3084–85 (creating an opt-out system for expunging DNA profiles from the national index and authorizing collection of DNA samples from persons arrested or detained under federal law).

75. Patrick J. Rauss et al., *FERET (Face Recognition Technology) Program*, 2962 PROC. SPIE 253, 253 (1997), *available at* http://adsabs.harvard.edu/abs/1997SPIE.2962..253R.

76. *Face Recognition Vendor Test*, NIST INFO. TECH. LABORATORY, http://www.nist.gov/itl/iad/ig/frvt-home.cfm (last visited Nov. 2, 2012).

77. *See* P. JONATHON PHILLIPS ET AL., FERET (FACE RECOGNITION TECHNOLOGY) RECOGNITION ALGORITHM DEVELOPMENT AND TEST RESULTS 9, 33 (1996), *available at* http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.19.3924.

78. BIOMETRICS IN GOVERNMENT POST-9/11, *supra* note 38, at 9, 24.

the Human Identification at a Distance (HumanID) Program.[79] DARPA reported that the purpose of the program was to provide early warning support for force protection and homeland security against terrorism and crime.[80] The goal was to develop algorithms for locating and acquiring subjects up to 150 meters (500 feet) away, fusing face and gait recognition into a 24/7 human identification system.[81] (This program transferred to the Information Awareness Office post-9/11 and formed one component of John Poindexter's Total Information Awareness program.)[82] At the conclusion of FERET, DoD's Counterdrug Technology Development Program Office, DARPA, and the National Institute of Justice created a facial recognition vendor test to keep abreast of commercial developments in the field.[83]

In 1995, the INS similarly launched a facial (and voice) recognition program, narrowly focused on individuals crossing the Mexico-U.S. border at Otay Mesa, California.[84] The following year Congress extended the so-called SENTRI program (Secure Electronic Network for Travelers Rapid Inspection), to Laredo, Hidalgo, and El Paso, Texas, as well as Nogales and San Louis, Arizona.[85] SENTRI rapidly expanded to the northern

79. *Id.* at 9, 18.

80. *Human ID at a Distance (HumanID)*, INFO. AWARENESS OFFICE, http://infowar.net/tia/www.darpa.mil/iao/HID.htm (last visited Nov. 2, 2012).

81. *Id*.

82. *See* GINA MARIE STEVENS, CONG. RESEARCH SERV., RL 31730, PRIVACY: TOTAL INFORMATION AWARENESS PROGRAMS AND RELATED INFORMATION ACCESS, COLLECTION, AND PROTECTION LAWS (2003), *available at* http://www.fas.org/irp/crs/RL31730.pdf.

83. FACIAL RECOGNITION VENDOR TEST 2000, EVALUATION REPORT 12 (2001), *available at* http://www.face-rec.org/vendors/FRVT_2000.pdf. There have since been four occasions on which similar tests were conducted to evaluate publicly-available products. *See Face Recognition Vendor Test*, NIST INFO. TECH. LABORATORY (JULY 31, 2012), http://www.nist.gov/itl/iad/ig/frvt-home.cfm.

84. *See* BIOMETRICS IN GOVERNMENT POST-9/11, *supra* note 38, at 8, 23 (noting use of facial and voice recognition at Otay Mesa, California border crossing); *see also SENTRI Program Description*, CPB.GOV, http://www.cbp.gov/xp/cgov/travel/trusted_traveler/sentri/sentri.xml (last visited Nov. 2, 2012) [hereinafter *SENTRI*] (providing a description of the SENTRI program, including eligibility criteria).

85. *Inspection of the Secure Electronic Network for Travelers' Rapid Inspection: Appendix II*, U.S. DEP'T OF JUSTICE (June 2000), http://www.justice.gov/oig/reports/INS/e0019/app2.htm (providing a timeline of major project milestones, including the October 1996 federal regulations allowing collection of user fees for pilot program). For the current SENTRI enrollment centers see *SENTRI*, *supra* note 84.

border.[86] The highly visible initiative generated a number of awards for the use of innovation and technology in government.[87]

What these and other programs suggest is that, prior to 9/11, movement within specific biometric areas, such as fingerprint, DNA, and facial recognition, paralleled growing interest in biometrics generally. It took the attacks, however, to catapult these programs to special status. Myriad federal, state, and local programs followed, in the process significantly blurring the lines between investigations and intelligence gathering and giving rise to concern about the use of remote biometric identification.

B. POST-9/11 FEDERAL BIOMETRIC AND FACIAL IDENTIFICATION PROGRAMS

Almost immediately following the attacks, Congress made it clear that it expected movement in the biometric realm and made substantial resources available for the purpose.[88] The Executive mirrored the legislature: the White House issued directives targeting the development of biometric technologies. Almost every major department tasked with national security and law enforcement initiated some sort of biometric activity. The Department of Homeland Security, Department of Justice, Department of State, Department of Defense, and Department of Health and Human Services each created new biometric programs.

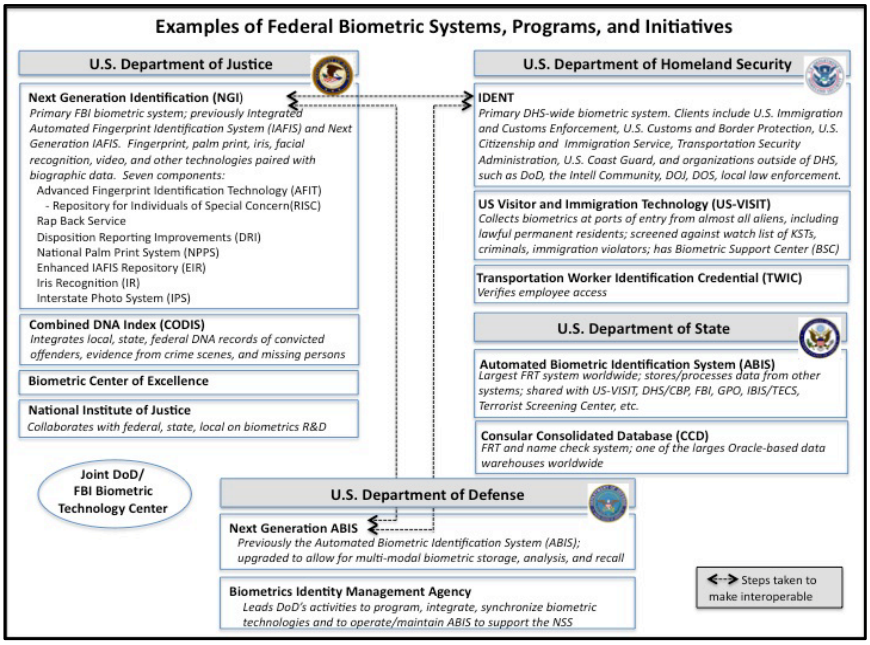
86. *See, e.g.*, *Inspection of the Secure Electronic Network for Travelers' Rapid Inspection: Memorandum from Robert L. Ashbaugh, Acting Inspector Gen., to Doris Meissner, Comm'r, Immigration and Naturalization Serv.*, U.S. DEP'T OF JUSTICE (June 20, 2000), http://www.justice.gov/oig/reports/INS/e0019/exec.htm (listing the Peace Bridge in Buffalo, New York and Ambassador Bridge in Detroit, Michigan as SENTRI sites).

87. *See Inspection of the Secure Electronic Network for Travelers' Rapid Inspection: Appendix II*, *supra* note 85 (noting SENTRI was the Vice President's National Performance Review Hammer Award winner—granted to teams of federal employees making significant contributions towards reinventing government principles—in October 1996, selected for inclusion in the Smithsonian Institute's Permanent Research Collection as part of the Computerworld Smithsonian Awards Program in June 1997, and a semifinalist in the Innovations in American Government award program, jointly sponsored by the Ford Foundation and Harvard University in October 1998).

88. In addition to the statutory initiatives, discussed *infra*, see *Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism: Hearing Before the Subcomm. on Tech., Terrorism, and Gov't Info. of the Comm. on the Judiciary*, 107th Cong. 24 (2001) (touting the benefits of facial recognition and downplaying concerns about accuracy).

Initially, focus centered on individuals entering and leaving the United States, as well as on those working in secure transportation areas.[89] Emphasis quickly expanded to other areas, such as government employee identification, domestic law enforcement, intelligence gathering, surveillance, military targeting, and confirmation of the identity of individuals killed as part of war.[90] The nature of the technologies sought expanded from IBI to RBI, in the process raising a new set of legal and constitutional questions. *Figure 2* provides some examples of the current systems, programs, and initiatives, discussed in the ensuing text.

Figure 2



1. Border Security

Prior to 9/11, Congress enacted several statutory provisions requiring the Executive Branch to create a more robust

89. *See, e.g.*, GOV'T ACCOUNTABILITY OFFICE, GAO-04-785T, AVIATION SECURITY: CHALLENGES IN USING BIOMETRIC TECHNOLOGIES 12–17 (2004), *available at* http://www.gao.gov/new.items/d04785t.pdf.

90. Because many of the programs involved more than one identification technology in their design and implementation, I adopt an approach in the following section based on the purpose of the programs. At least some of the technologies incorporated represent IBI, not RBI; however, the inclusion of RBI-type technologies moves the categorization of the programs to the RBI realm.

entry and exit program for foreign visitors to the United States.[91] Following the attacks, the matter became more urgent, with increasing focus on the potential role of technology in creating a more accurate and efficient system. The immediate emphasis stemmed from concern that the nineteen hijackers passed directly through airport security on the day of the attacks, as well as through immigration screening during their previous entry to the United States.[92] Eighteen of the nineteen, moreover, had been issued U.S. identification documents.[93] Recognizing potential terrorists, though, was like finding a needle in a haystack: with more than 300 formal ports of entry, some half a billion annual crossings were taking place.[94] As for documentation, the Department of State processed more than 9 million visa applications annually, with the DHS considering another 50,000 requests for asylum per year, and 30,000 applications for immigration benefits *per day*.[95] The question of how to address security concerns was complicated by the country's economic and commercial interests. The economy depended upon the quick and efficient movement of people and goods across the borders. New technologies offered a solution and multiple initiatives followed.

Three points about these programs deserve notice: first, each has rapidly expanded its reach, in the process creating the largest worldwide repository of images subject to facial recognition technology; second, emphasis has been placed not just on data accumulation, but on information sharing between federal agencies; and third, even within border security, the federal government has increasingly invested in RBI technologies to supplement its IBI capabilities.

Congress has played a key role in encouraging the Executive Branch to move into this area. The USA PATRIOT Act, for instance, directed the Attorney General and the Secretary of State jointly, through the National Institute of Standards Technology, to develop and certify a technology standard that

91. *See, e.g.*, Visa Waiver Permanent Program Act of 2000, Pub. L. No. 106-396, § 205, 114 Stat. 1637, 1641–43; Immigration and Naturalization Service Data Management Improvement Act of 2000, Pub. L. No. 106-215, § 2, 114 Stat. 337, 337–39.

92. BIOMETRICS IN GOVERNMENT POST-9/11, *supra* note 38, at 6.

93. *Id.*

94. *Id.* at 28.

95. *Id.*

could be used to verify visa applicants' identities.[96] The object was to develop a cross-agency, cross-platform system for sharing law enforcement information and intelligence.[97] The legislature directed that the system be easily accessible to all consular officers overseeing visa applications, all federal inspection agents at the border, and all law enforcement and intelligence officers related to the admission of aliens into the United States.[98] The legislation went on to discuss biometrics in particular, requiring the Attorney General, in consultation with the Secretary of State and the Secretary of Transportation, to conduct a study on the feasibility of using biometric identifier systems with access to the FBI's IAFIS at consular offices overseas and at U.S. borders.[99] In 2002, the Enhanced Border Security and Visa Entry Reform Act took the technology a step further. The legislation required that all persons applying for visas have fingerprints and digital photographs collected during the visa application interview.[100] The information must be cleared through IDENT prior to a visa being granted.[101] The State Department subsequently initiated a Biometric Visa Program, enabling overseas posts to install the necessary hardware and software.[102]

White House interest in using technology to solve the problem reflected Congress's approach.[103] Homeland Security Presi-

96. USA PATRIOT Act, Pub. L. No. 107-56, § 403(c)(1), 115 Stat. 272, 344 (2001).

97. *Id.* § 403(c)(2), 115 Stat. at 344.

98. *Id.* § 403(c)(3), 115 Stat. at 344.

99. *Id.* § 1008(a), 115 Stat. at 395. The subsequent report, due within ninety days, was to be submitted to the Committee on International Relations, the Committee on the Judiciary of the House of Representatives, the Committee on Foreign Relations, and the Committee on the Judiciary of the Senate. *Id.* § 1008(b), 115 Stat. at 395.

100. *See* Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. No. 107-173, § 303(b)(2), 116 Stat. 543, 553.

101. GOV'T ACCOUNTABILITY OFFICE, GAO-04-1001, BORDER SECURITY: STATE DEPARTMENT ROLL OUT OF BIOMETRIC VISAS ON SCHEDULE, BUT GUIDANCE IS LAGGING 1 (2004), *available at* http://www.gao.gov/assets/250/244011.pdf.

102. BIOMETRICS IN GOVERNMENT POST-9/11, *supra* note 38, at 9.

103. Pursuant to Executive Order 13228, October 8, 2001, the Bush Administration established two new bureaucratic agencies: the Office of Homeland Security (lodged within the Executive Office of the President), and the Homeland Security Council (HSC), which was chaired by the President. HAROLD C. RELYEA, CONG. RESEARCH SERV., RS 22840, ORGANIZING FOR HOMELAND SECURITY: THE HOMELAND SECURITY COUNCIL RECONSIDERED 1 (2008) *available at* http://fpc.state.gov/documents/organization/103696.pdf. On October 29, 2001, the HSC held its first meeting; simultaneously, the President announced

dential Directive (HSPD) 6 laid out the framework for developing a terrorism screening program, requiring that the Attorney General, Secretary of State, Secretary of Homeland Security, and Director of Central Intelligence submit information to the Terrorist Threat Integration Center.[104] A consolidated Terrorist Screening Center Database would collect and correlate data for use in quickly identifying potential threats. HSPD-11 subsequently established a more comprehensive approach to terrorist screening, even as it specified that the information obtained by the center take account of biometric identifiers.[105] National Security Presidential Directive 59/HSPD-24 later squarely addressed federal coordination of the collection, storage, use, analysis, and sharing of biometric and associated biographic

the creation of HSPDs to "record and communicate presidential decisions about the homeland security policies of the United States." *Id.* at 2. Like the equivalent documents for the National Security Council, the first directive outlined the organization and operation of the HSC. *Id.* The second, issued the same day, detailed immigration policies, and the third such document, which followed nearly five months later, created the Homeland Security Advisory System. *Id.* Over the course of the two administrations, twenty-three HSPDs were issued, some of which were classified and some of which were concurrently issued as National Security Presidential Directives. *Id.* The unclassified documents, published in the *Weekly Compilation of Presidential Documents*, were neither published in the *Federal Register* nor reproduced in the *Public Papers of the Presidents of the United States*. *Id.* at n.7; *see also* HAROLD C. RELYEA, CONG. RESEARCH SERV., 98-611 GOV, PRESIDENTIAL DIRECTIVES: BACKGROUND AND OVERVIEW 6–7 (2008), *available at* http://www.fas.org/irp/crs/98-611.pdf. Upon passage of the Homeland Security Act on November 25, 2002, a reconstituted HSC, located within the Executive Office of the President, became responsible for providing advice to the President on matters involving homeland security, including overseeing and reviewing federal homeland security policies. REYLEA, *supra*, at 3.

104. Homeland Security Presidential Directive/HSPD-6, Integration and Use of Screening Information to Protect Against Terrorism, 39 WEEKLY COMP. PRES. DOC. 1174 (Sept. 16, 2003) [hereinafter HSPD-6], *available at* http://www.gpo.gov/fdsys/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1174.pdf. Homeland Security Presidential Directives, initiated in the wake of 9/11, focus on matters related to homeland security. *See National Security Presidential Directives [NSPD]*, FEDERATION AM. SCIENTISTS, http://www.fas.org/irp/offdocs/nspd/index.html (last visited Nov. 2, 2012) (listing both National Security Presidential Directives and Homeland Security Presidential Directives). As of the time of writing, twenty-five such documents have issued. *Id.*

105. *See* Homeland Security Presidential Directive/HSPD-11: Comprehensive Terrorist-Related Screening Procedures, 40 WEEKLY COMP. PRES. DOC. 1709 (Aug. 27, 2004), *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2004/08/20040827-7.html; *see also Biometrics: A Decade of Progress Since 9/11: Maturation of Federal Biometric Activities*, FBI BIOMETRIC CENTER OF EXCELLENCE (2011), http://www.biometriccoe.gov/Resources/Online_Library.htm.

and contextual information of "known and suspected terrorists."[106]

Numerous departmental programs followed the lead set by Congress and the White House. In March 2003, for example, responsibility for U.S. ports of entry by air, land, or sea transferred from the former INS to DHS.[107] In consultation with the Department of State (DOS), DHS established U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT), an automated system aimed at foreign nationals.[108] In 2004, the program began integrating biometrics from non-citizens collected at international ports of entry.[109]

These programs appear to collect a significant amount of information and, through their use of biometric identification, generate new knowledge. This runs somewhat counter to agency claims. DHS asserts, for example, that US-VISIT is not a single system or database, saying instead that it "integrates and enhances" existing systems and allows for interface with other DHS agencies, DOS, and others.[110] Nevertheless, the program itself collects data directly from travelers.[111] Although DHS stated at the inception of the program that it did not anticipate that the program would use data mining technology, nothing in the original design prevents this from occurring.[112]

106. Press Release, The White House, Homeland Security Presidential Directive/ HSPD-24: Biometrics for Identification and Screening to Enhance National Security (June 5, 2008) [hereinafter HSPD-24], *available at* http://www.biometrics.gov/Documents/NSPD59%20HSPD24.pdf.

107. GOV'T ACCOUNTABILITY OFFICE, GAO-07-248, BORDER SECURITY: US-VISIT PROGRAM FACES STRATEGIC, OPERATIONAL, AND TECHNOLOGICAL CHALLENGES AT LAND PORTS OF ENTRY 1 (2006) [hereinafter GAO, US-VISIT], *available at* http://www.gao.gov/new.items/d07248.pdf.

108. *Id.* US-VISIT is operated by a special program office that reports to the DHS Deputy Secretary and is used by U.S. Customs and Border Protection, to whom responsibility for U.S. immigration laws governing the admissibility of aliens, cargo, agriculture, and animals has been given. *Id.* at 1–2.

109. BIOMETRICS IN GOVERNMENT POST-9/11, *supra* note 38, at 9.

110. U.S. DEP'T OF HOMELAND SEC., UPDATED PRIVACY IMPACT ASSESSMENT FOR THE UNITED STATES VISITOR AND IMMIGRANT STATUS INDICATOR TECHNOLOGY (US-VISIT) PROGRAM: INTERNATIONAL LIVE TEST—PHASE II: TESTING OF ICAO-COMPLIANT E-PASSPORTS FROM SELECTED COUNTRIES 2 (2005) [hereinafter PHASE II], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_update_12-22-2005.pdf.

111. The information includes name, date of birth, gender, country of citizenship/nationality, passport number, country of issuance, travel document type, date of issuance, U.S. destination address, arrival and departure information, a digital photograph, digital fingerscans, and, in some cases, unique and individually assigned RFID tag numbers. *Id.* at 3.

112. *Id.* at 7.

DHS, moreover, simultaneously noted that the information would be shared with other agencies,[113] many of which make use of data mining technologies. The program, in turn, draws on other agencies' databases and watch lists.[114]

US-VISIT has steadily expanded over time.[115] Initially focused on entry data, in 2004, the Intelligence Reform and Terrorism Prevention Act required the collection of biometric *exit* data for all individuals subject to US-VISIT.[116] Implementation of this requirement has been delayed, principally owing to feasibility and limited resources.[117] There has been some effort to address the issue through further use of technology: namely, embedding radio-frequency identification (RFID) chips in I-94 Arrival/Departure forms, thus allowing the government to record individuals departing from the country using RFID readers mounted on posts.[118] The system, which has been erected along certain points of entry along the southern border, has been less than effective, owing in some measure to the failure

113. *Id.* at 10. DHS shares both biometric and biographic information collected by the program with DOS, DOJ/FBI, DoD, and "other agencies at the [f]ederal, state, local, foreign, or tribal level who are lawfully engaged in collecting law enforcement information (whether civil or criminal) and national security intelligence information." *Id.* Note that data mining itself also lacks a legal framework. For discussion of this point and a list of national security data mining programs in this area, see Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435 (2008); *see also Defense of Privacy Act and Privacy in the Hands of the Government: Joint Hearing on H.R. 338 Before the H. Comm. on the Judiciary, Subcomm. on Commercial and Admin. Law and the Subcomm. on the Constitution*, 108th Cong. 17–24 (2003) (statement of James X. Dempsey, Exec. Dir., Ctr. for Democracy & Tech.) (drawing attention to the absence of effective legislation on data mining techniques).

114. *See* GAO, US-VISIT, *supra* note 107, at 16–17; *US-VISIT Biometric Requirements to Include Legal Permanent Residents*, LAB. IMMIGR. L. (Dec. 18, 2008), http://www.laborimmigration.com/2008/12/us-visit-biometric-requirements-to-include-legal-permanent-residents. This includes, inter alia, comparing the information from the applicant to data stored in IDENT. Enrollment of Additional Aliens in US-VISIT; Authority to Collect Biometric Data From Additional Travelers and Expansion to the 50 Most Highly Trafficked Land Border Ports of Entry, 73 Fed. Reg. 77,473, 77,477–78 (Dec. 19, 2008) (to be codified at 8 C.F.R. pts. 215, 235).

115. For a discussion of the incremental expansion of the program see U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT UPDATE FOR THE US-VISIT PROGRAM 4 (2005) [hereinafter DHS, UPDATE FOR US-VISIT], *available at* http://epic.org/privacy/surveillance/spotlight/0905/usv_pia3.pdf.

116. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 7208, 118 Stat. 3817, 3817–23.

117. GAO, US-VISIT, *supra* note 107, at 39.

118. *Id.* at 44.

of the readers to perceive RFID chips in passing vehicles, and the placement of the posts on nearby hillsides—not along the sidewalks being used by pedestrians leaving the country.[119]

The number of individuals whose biometric information has been collected by US-VISIT has exponentially increased as additional classes of travelers have been added to the program. Initially, U.S. citizens and lawful permanent residents were exempt from US-VISIT, as were certain non-citizens.[120] In 2006, DHS expanded the system to include additional classes of aliens and to enable the database to receive information not just directly from travelers, but also from the U.S. Citizens and Immigration Service Image Storage and Retrieval System/Biometric Support System.[121] In 2009, DHS further expanded the system, issuing a new rule that extended the program to nearly all aliens, including lawful permanent residents (with an exception for Canadian citizens seeking short-term business or pleasure, or individuals traveling on A and G visas).[122]

Between the program's inception in January 2004 and the final rule change of January 2009, the program screened more than 130 million aliens when they applied for admission to the United States.[123] DHS claims that the program has been suc-

119. *Id.* at 46–51.

120. Privacy Impact Assessment and Privacy Policy Notice, 69 Fed. Reg. 2608, 2614 (Jan. 16, 2004); U.S. DEP'T OF HOMELAND SEC., UNITED STATES VISITOR AND IMMIGRANT STATUS INDICATOR TECHNOLOGY (US-VISIT) PROGRAM 3 (2006) [hereinafter DHS, VISITOR AND IMMIGRANT STATUS], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_addaliens.pdf; DEP'T OF HOMELAND SEC., US-VISIT INCREMENT 2C PROOF OF CONCEPT (2005), *available at* http://www.dhs.gov/xlibrary/assets/usvisit/US-VISIT_2CPOCCONOPSPhase1.pdf; U.S. DEP'T OF HOMELAND SEC., US-VISIT PROGRAM, INCREMENT 2, PRIVACY IMPACT ASSESSMENT 13 (2004) [hereinafter DHS, INCREMENT 2], *available at* http://epic.org/privacy/us-visit/us-visit_pia2.pdf; *see also* U.S. DEP'T OF HOMELAND SEC., US-VISIT PROGRAM PRIVACY IMPACT ASSESSMENT UPDATE: INTERNATIONAL LIVE TEST 10 (2005), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_livetest.pdf; PHASE II, *supra* note 110, at 6.

121. DHS, VISITOR AND IMMIGRANT STATUS, *supra* note 120, at 2.

122. *See* Enrollment of Additional Aliens in US-VISIT; Authority to Collect Biometric Data from Additional Travelers and Expansion to the 50 Most Highly Trafficked Land Border Ports of Entry, 74 Fed. Reg. 2,837, 2837 (Jan. 16, 2009) (to be codified at 8 C.F.R.§ 235.1).

123. Enrollment of Additional Aliens in US-VISIT; Authority to Collect Biometric Data From Additional Travelers and Expansion to the 50 Most Highly Trafficked Land Border Ports of Entry, 73 Fed. Reg. 77,473–74 (Dec. 19, 2008) (to be codified at 8 C.F.R. pts. 215, 235). Note that most persons entering the United States enter through land ports of entry. GOV'T ACCOUNTABILITY OF-

cessful, citing adverse action taken against more than 3,800 aliens based on information obtained through the US-VISIT biometric screening process.[124] DHS, however, defines "adverse action" rather broadly—namely, denial of admission, expedited removal, general detention, or arrest pursuant to a criminal arrest warrant.[125] It is not clear whether the biometric element of the programs has substantially altered security at the border.

Efforts to strengthen DHS's underlying database, IDENT, continued post-9/11, prompting the department to issue a new Privacy Impact Assessment (PIA).[126] Unlike the original INS database, which focused on INS's area of responsibilities, the integration of INS into DHS brought with it a correspondingly broader application for the information.[127] DHS does not just focus on immigration and naturalization; it is responsible for all of homeland security.[128] Accordingly, by 2007 IDENT had become "the primary DHS-wide system for the biometric identification and verification of individuals encountered in DHS mission-related processes."[129] This meant that biometric data was now paired with biographical and encounter data contributed by a wide range of organizations, such as U.S. Immigration and Customs Enforcement, U.S. Customs and Border Protection, U.S. Citizenship and Immigration Service, Transportation Se-

FICE, GAO-07-499T, HOMELAND SECURITY: US-VISIT HAS NOT FULLY MET EXPECTATIONS AND LONGSTANDING PROGRAM MANAGEMENT CHALLENGES NEED TO BE ADDRESSED 5 (2007) [hereinafter GAO-07-499T HOMELAND SECURITY], *available at* http://www.gao.gov/new.items/d07499t.pdf. In fiscal year 2004, for instance, 335.3 million entered via land ports, 75.1 million through air ports, and 14.7 million via sea ports. *Id.* at 7. A greater percentage of aliens, however, are processed at air ports of entry. *Id.* In fiscal year 2004, for instance, only 1.4% of those entering through land ports were processed through US-VISIT, with 42.2% of those entering through air ports and 38.8% of those arriving into sea ports being processed by US-VISIT. *Id.*

124. GAO-07-499T HOMELAND SECURITY, *supra* note 123, at 10.

125. Enrollment of Additional Aliens in US-VISIT; Authority to Collect Biometric Data from Additional Travelers and Expansion to the 50 Most Highly Trafficked Land Border Ports of Entry, 73 Fed. Reg. at 77,474.

126. *See* U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT) (2006) [hereinafter DHS, IDENT 2006], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_ident_final.pdf. See discussion *infra* Part II.A.5 for more detail on the statutory framing for PIAs.

127. *See* DHS, IDENT 2006, *supra* note 126, at 2.

128. *Id.*

129. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT UPDATE FOR THE ENUMERATION SERVICES OF THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT) 2 (2007), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_enumeration.pdf.

curity Administration, and the U.S. Coast Guard, as well as organizations outside of DHS, such as the State Department, DOJ, FBI, DoD, "and other governmental organizations that collaborate with DHS in pursuing DHS national security, law enforcement, immigration, intelligence, and other DHS mission-related functions."[130] DHS, in turn, began sharing the information with federal, state, local, tribal, foreign, or international government agencies, as well as contractors.[131]

The new PIA noted that for DHS's security purposes special conditions would henceforth apply—notice, for instance, may not be provided to the individual prior to the collection of information in either a national security or law enforcement context.[132] In similar fashion, the opportunity or right to decline to provide information in such contexts may be nonexistent.

> Whether an individual has a right to consent to a particular use of their data depends on the purpose of the collection . . . . [I]n most cases, because of the DHS national security, law enforcement, immigration, or DHS-mission related purposes for which the information is collected, no such right exists.[133]

Information collected under IDENT can be retained for up to seventy-five years.[134]

To assist IDENT in its functions, DHS created a biometric watch list.[135] It also anticipated the creation of new biometrics databases that would feed into other systems, such as the Treasury Enforcement Communications System (TECS).[136] Additionally, DHS initiated a program called Secure Communities—essentially an immigrant fingerprinting program, in which FBI prints from booked offenders are run against IDENT

130. DHS, IDENT 2006, *supra* note 126, at 3.

131. Such transfers are governed by memoranda of understanding or other interagency security agreements. *Id.* at 9 (outlining contributors); *id.* at 13 (discussing contractors).

132. *Id.* at 10.

133. *Id.* at 10–11.

134. PHASE II, *supra* note 110, at 8.

135. *See* U.S. DEP'T OF HOMELAND SEC., US-VISIT PROGRAM, INCREMENT 1, PRIVACY IMPACT ASSESSMENT 4 (2003) [hereinafter DHS, INCREMENT 1], *available at* http://epic.org/privacy/us-visit/us-visit_pia.pdf. Note that the initial privacy impact assessment was published in the *Federal Register* of January 4, 2004, but was subsequently amended to correct a technical error (incorrect telephone number). *See* Privacy Impact Assessment and Privacy Policy Notice, 69 Fed. Reg. 2,608, 2,611 (Jan. 16, 2004).

136. *See* DHS, INCREMENT 1, *supra* note 135, at 4.

to find out whether they are in the country illegally.[137] In 2007, the Coast Guard began submitting fingerprints from migrants against the FBI's IAFIS, DHS's IDENT, and DoD's ABIS.[138]

In addition to the above initiatives, following 9/11, the U.S. Citizenship and Immigration Services (USCIS), part of DHS, integrated biometrics into its immigration benefits system.[139] The Department created what is called the Biometric Storage System, with the aim of creating a centralized repository of all biometric data captured by USCIS from applicants filing immigration applications.[140] Ten-print fingerprint and associated biographic information for biometric-based background checks on those applying or petitioning for immigration benefits are included.[141] Biographic data includes the Alien Registration Number, first and last name, date and country of birth, gender, aliases, height, weight, race, class of admission, address, as well as other biographic information.[142]

INS's initial objections to ten-print capture and analysis were soon replaced (in a post-9/11 environment) by a ten-print standard. In 2006, the State Department similarly deployed a ten-print pilot program.[143] By the following year, all State Department visa-issuing points had adopted ten-print collections.[144] Also in 2007, DHS US-VISIT began collecting ten-prints at all U.S. airports and U.S. Customs and Border Protection (CBP) ten-prints for full search against the FBI Criminal Master File. The same year, USCIS similarly moved to a ten-print system for its Biometric Storage System.[145]

Outside of DHS, the Department of State maintains two major biometric databases: the Consular Consolidated Database (CCD) and the Automated Biometric Identification System. The former, CCD, is one of the largest Oracle-based data

137. Aliya Sternstein, *FBI to Launch Nationwide Facial Recognition Service*, NEXTGOV, Oct. 7, 2011, http://www.nextgov.com/technology-news/2011/10/fbi-to-launch-nationwide-facial-recognition-service/49908.

138. *Biometrics: A Decade of Progress Since 9/11*, *supra* note 105.

139. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE BIOMETRIC STORAGE SYSTEM 2 (2007) [hereinafter DHS, BIOMETRIC STORAGE SYSTEM], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_bss.pdf.

140. *Id.*

141. *Id.*

142. *Id.* at 4.

143. *Biometrics: A Decade of Progress Since 9/11*, *supra* note 105.

144. *Id.*

145. DHS, BIOMETRIC STORAGE SYSTEM, *supra* note 139, at 2.

warehouses in the world. As of December 2009, it contained over 100 million visa case files and 75 million photographs, with some 35,000 cases added per day.[146] The CCD provides a gateway to IDENT (discussed *supra* Part I.A.) and IAFIS/IAFIT (discussed *supra* Part I.A.), as well as the Department of State Facial Recognition system and the NameCheck system.[147] It stores biographic and biometric information about U.S. persons (citizens and lawful permanent residents), as well as foreign nationals.[148] While some of the information is provided by applicants, other information (such as names, addresses, birth dates, race, identification numbers, and country of origin) is obtained via commercial databases or public records.[149] The data is used to screen applicants, register facial images for FRT, and report on particular applicants.[150] The information is shared with a number of external agencies and programs, such as US-VISIT, DHS/CBP, Army Intelligence and Security Command, the FBI, the Government Printing Office, the DHS Interagency Border Inspection/Treasury Enforcement Control System, the DHS Terrorist Screening Center, and others.[151] Because the CCD is a data warehouse used to store and process data collected by other systems and does not collect information directly from individuals, it is not required to provide notice of the purpose, use, or authority of the collection of information.[152]

In June 2011, DOS issued a PIA for its Automated Biometric Identification System, a facial recognition program designed to help the State Department evaluate visa and passport applications.[153] The system is designed to recognize several photos of the same person in different databases on a scale "expo-

146. U.S. DEP'T OF STATE, CONSULAR CONSOLIDATED DATABASE (CCD) PRIVACY IMPACT ASSESSMENT (PIA) 1 (2010) [hereinafter CONSULAR CONSOLIDATED DATABASE (CCD) PIA], *available at* http://www.state.gov/documents/organization/93772.pdf.

147. *Id.*

148. *Id.* at 2.

149. *Id.* at 6.

150. *Id.* at 5–6.

151. *Id.* at 14–16.

152. *Id.* at 17.

153. Note that ABIS is a commercially available off-the-shelf product developed by a private company, L-1 Identity Solutions. U.S. DEP'T OF STATE, AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (ABIS) PRIVACY IMPACT ASSESSMENT 1 (2011), *available at* http://www.state.gov/documents/organization/109132.pdf.

nentially larger than those which a human could review."[154] ABIS incorporates databases relating to visa, passport, Watchlist Gallery, and Passport Lookout Tracking System images, making it, according to the State Department, "the largest facial recognition system deployed in the world."[155]

ABIS grew directly from the USA PATRIOT Act and the Enhance Border Security and Visa Entry Reform Act demands positive identification of visa applicants.[156] By 2011, the FRT system contained records on over 139 million individuals.[157] It is expected to grow to 210 million person records by 2012, with approximately 25 million additional records added annually in subsequent years.[158] The system was designed to include not only face templates, but also demographic data, such as date of birth, gender, and place of birth.[159] The Department of State notes that the retention of the information depends upon the specific type of record, with no further details provided.[160]

Interestingly, the State Department does not actually own the system. Instead, it leases it from a private company, which means that both government employees and contractors have access to the information.[161] As with many aspects of the biometrics infrastructure, the government is heavily dependent upon non-governmental, for-profit businesses, subject to different rules than government agencies. Potential misuse of the system, DOS notes, includes not just delays in processing applications, but blackmail, identity theft or assumption, account takeover, physical harm, discrimination, and emotional distress. Improper use may further lead to financial loss, loss of public reputation and public confidence, and civil liability for the Department of State.[162]

2. Authentication

Along with the identification of individuals traveling across U.S. borders, the 9/11 attacks spurred new initiatives focused

154. *Id.*
155. *Id.* The Watchlist Gallery includes photos from the National Counterterrorism Center. *Id.* at 3.
156. *See id.* at 2.
157. *Id.* at 3.
158. *Id.*
159. *Id.* at 2–4, 6.
160. *Id.* at 6.
161. *See id.* at 4–5.
162. *Id.* at 4.

on authenticating the identity of transportation workers, government employees, and military personnel with access to secure areas. Most of these initiatives appear to be designed with immediate biometric identification in mind; the widespread collection of such data, however, when paired with video technologies, allows for expansion into the realm of remote biometric identification.

The Federal Aviation Administration, for instance, with the support of the Department of Defense, created the Aviation Security Biometrics Working Group.[163] It had less than two months to consider the efficacy of integrating biometric technologies into the nation's airport security infrastructure.[164] Of particular concern was the role the federal government could play in advancing technology to ensure the development of new and effective systems. Interoperability across agencies would be critical.[165]

Congress kept step with the Executive. The Aviation and Transportation Security Act, enacted in November 2001, required federal cooperation with airport operators to strengthen access control in secured areas and to consider using biometric access control systems to verify identity.[166] The following year, Congress passed two new laws, incorporating biometric technology into cross-border functions: the Enhanced Border Security and Visa Entry Reform Act of 2002[167] and the Maritime Transportation Security Act of 2002 (MTSA).[168] The latter statute embraced the Transportation Worker Identification Credential (TWIC), requiring that it contain biometric information to help regulate unescorted access to all MTSA secure areas.[169] In 2007, TWIC enrollment and issuance began.[170]

163. GOV'T ACCOUNTABILITY OFFICE, GAO-04-785T, AVIATION SECURITY: CHALLENGES IN USING BIOMETRIC TECHNOLOGIES 12 (2004), *available at* http://www.gao.gov/new.items/d04785t.pdf; BIOMETRICS IN GOVERNMENT POST-9/11, *supra* note 38, at 7.

164. BIOMETRICS IN GOVERNMENT POST-9/11, *supra* note 38, at 7.

165. *See id.*

166. Aviation and Transportation Security Act, Pub. L. No. 107-71, § 106(a), 115 Stat. 597, 609 (2001) (codified as amended at 49 U.S.C. § 114).

167. Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. No. 107-173, § 202(a)(4)(B)(i), 116 Stat. 543, 549 (codified as amended in scattered sections of 8 U.S.C.).

168. Maritime Transportation Security Act of 2002, Pub. L. No. 107-295, § 102, 116 Stat. 2064, 2073.

169. *Id.*; *see also* GOV'T ACCOUNTABILITY OFFICE, GAO-08-1151T, TRANSPORTATION SECURITY: TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL: A STATUS UPDATE 1 (2008), *available at* http://www.gao.gov/new.items/

In 2004, HSPD-12 required the development of new standards to govern identity cards granting access to federal government locations and systems.[171] The Federal Information Security Management Act of 2002 authorized the Chief Information Officers Council, in conjunction with the National Institute of Standards and Technology, to develop recommendations on information technology standards.[172] The Personal Identity Verification (PIV) standard for Federal Employees and Contractors and the Federal Information Processing Standard (FIPS 201) established standards for identity credentials[173] and required that biometric information be included in the PIV card.[174] A number of departments subsequently began using biometrics as part of their identity management systems. In 2009, the Department of State, for instance, issued a PIA for changes to its Identity Management System, a database storing the information collected from persons requiring personal ID cards.[175] Biometric information was one of a series of categories

d081151t.pdf (statement of Stephen M. Lord, Acting Dir., Homeland Sec. & Justice Issues).

170. BIOMETRICS IN GOVERNMENT POST-9/11, *supra* note 38, at 10.

171. Directive on Policy for a Common Identification Standard for Federal Employees and Contractors: Homeland Security Presidential Directive/HSPD -12, 40 WEEKLY COMP. PRES. DOC. 1709 (Aug. 27, 2004) [hereinafter HSPD-12], *available at* http://www.gpo.gov/fdsys/pkg/WCPD-2004-08-30/pdf/WCPD-2004-08-30-Pg1709.pdf.

172. Federal Information Security Management Act of 2002, Pub. L. 107-347, § 101, 116 Stat 2899, 2905–06 (codified as 44 U.S.C. § 3603). Note that in 2006, Congress passed the Security and Accountability For Every Port Act of 2006, amending MTSA to direct DHS to, inter alia, implement TWIC at the ten highest-risk ports by July 1, 2007. Security and Accountability For Every Port Act of 2006, Pub. L. No. 109-347, § 104, 120 Stat. 1884, 1888–91 (2006) (codified as 46 U.S.C. 70105(i)(2)(A)).

173. CHARLES WILSON ET AL., U.S. DEP'T OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., SPECIAL PUBLICATION 800-76-1, INFORMATION SECURITY iv (2007), *available at* http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf. This document is considered a companion document to FIPS 201. It covers the technical acquisition and specifications for formatting PIV biometric credentials, including the procedures and formats for facial images. The purpose of adopting clear criteria is to ensure universal interoperability and a high level of performance. Further information regarding biometric data suitable for FBI background investigations is included in SP 800-76. *Id.*

174. NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, FIPS PUB. 201-1, PERSONAL IDENTITY VERIFICATION (PIV) OF FEDERAL EMPLOYEES AND CONTRACTORS 33 (2006), *available at* http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.

175. U.S. DEP'T OF STATE, IDENTITY MANAGEMENT SYSTEM, PRIVACY IMPACT ASSESSMENT (2009) [hereinafter IDENTITY MANAGEMENT SYSTEM PRIVA-

of data that would be collected and potentially shared with other agencies.[176]

While many of these systems are designed to address authentication at the point of access, the accumulation of such information, if then paired with sequential recording (e.g., at multiple points of movement) or with video technologies, shifts the underlying considerations from IBI to RBI.

3. Investigations and Intelligence Gathering

Yet another area in which the post-9/11 era witnessed a movement into biometric technologies is in the realm of investigations and intelligence gathering. These initiatives blur the line between law enforcement and national security. The federalization of local information impacts the relationship of local and state authorities to the federal government. Perhaps most importantly, these initiatives move the government into a position where it can collect information (1) about multiple people; (2) from a distance; (3) in public space; (4) absent notice and consent; and (5) in a continuous and on-going manner—expanding the use of biometrics from immediate identification to RBI.

Following the attacks, the FBI's Biometric Center of Excellence quickly became a "hub for developing new and advanced biometric capabilities to solve crimes and protect national security."[177] Like the expansion of the INS biometric database to incorporate the breadth of the DHS mission, the FBI's enhanced national security role swept within it more applications, ranging from investigations to intelligence gathering, for which technology offered new opportunities. In addition to an expanding role for the FBI, the new context suggested the need for greater vertical and horizontal interoperability. As the FBI explained, "Criminal, Homeland Security, and Counterterrorism missions are converging and creating a need for greater integration of [law enforcement] and intelligence information among all levels of government."[178]

CY IMPACT ASSESSMENT], *available at* www.state.gov/documents/organization/122507.pdf.

176. *Id.* at 2, 4–5.

177. KIMBERLY J. DEL GRECO, FED. BUREAU OF INVESTIGATION, SEARCH ANNIVERSARY: THE NEXT 40 YEARS 10 (2009) [hereinafter SEARCH ANNIVERSARY], *available at* http://info.publicintelligence.net/FBI-CJISsearchbrief.pdf.

178. *Id.* at 12.

The first step was to expand IAFIS to include both classified and so-called "sensitive but unclassified" information in accordance with the Homeland Security Information Sharing Act.[179] Attorney General Ashcroft issued a memorandum that stated that the Department of Justice's overriding priority is the prevention of terrorist activity.[180] He ordered the FBI to expand its collection of counterterrorist information and directed the Legal Attaché Offices to obtain biometric information on all known or suspected foreign terrorists (KSTs) held by the Department of Defense and other federal agencies, as well as foreign entities.[181] Biometric and biographic information from these various sources was subsequently folded into IAFIS.

These changes radically expanded the database. By 2008, IAFIS housed "the largest collection of digital representations of fingerprint images, features from the digital fingerprint images, and criminal history information in the world."[182] At that point, it held information on more than 56.8 million people.[183] By 2009, this number had grown to at least 63.3 million subjects.[184] By February 2012, the database covered more than 72.9 million subjects.[185] According to the U.S. Census Bureau, the

179. 6 U.S.C. § 481 (2006).

180. *See* Press Release, Dep't of Justice, Attorney General Orders New Steps to Share Information Relating to Terrorism with Federal Agencies as well as State and Local Government (Apr. 11, 2002), *available at* http://www.justice.gov/opa/pr/2002/April/02_ag_211.htm.

181. *Privacy Impact Assessment: Integrated Automated Fingerprint Identification System National Security Enhancements*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/foia/privacy-impact-assessments/iafis (last visited Nov. 2, 2012).

182. *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS)*, *supra* note 18.

183. *Privacy Impact Assessment for the Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes—Channeling*, FED. BUREAU OF INVESTIGATION (May 5, 2008), http://www.fbi.gov/foia/privacy-impact-assessments/firs-iafis.

184. FED. BUREAU OF INVESTIGATION, CRIMINAL JUSTICE INFORMATION SERVICES DIVISION, NEXT GENERATION IDENTIFICATION 5 (2009) [hereinafter NEXT GENERATION IDENTIFICATION], *available at* http://www.search.org/files/pdf/DELANEY-Spring09.pdf.

185. *Integrated Automated Fingerprint Identification System: Fact Sheet*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis_facts (last updated Oct. 16, 2012). This massive fingerprint and data repository evolved to serve five functions. *Integrated Automated Fingerprint Identification System: Five Key Services*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis_services (last visited Nov. 2, 2012).

U.S. population is estimated to run around 312 million people.[186] This means that the Bureau holds fingerprint records on almost one-quarter of the U.S. population. Even allowing for a number of non-citizens in the database, this represents a significant percentage of the population. The acquisition of this information is heavily dependent on state and local police departments. (See discussion *infra* Part I.B.6).

IAFIS is not the only biometric database held by the FBI. Even as it expanded IAFIS, the Bureau began developing a new version of the database. Known initially as Next-Generation IAFIS, the initiative quickly became labeled Next Generation Identification. With this shift came an expansion in the use of biometric technologies from immediate identification to RBI. It also resulted in the incorporation of ever more records. The Government Accountability Office, for instance, puts the number of biometric records in the FBI's system at approximately ninety-four million.[187]

The problem the Bureau was trying to address in expanding its capabilities was anonymity—a condition that, from the Bureau's perspective, facilitated crime and created a national security threat.[188] The FBI argued, in particular, that increasingly sophisticated methods of masking identity demanded increasingly sophisticated methods of detecting it.[189] The current technologies proved insufficient. Behavioral biometrics, passwords, PINs, and ID cards easily could be bypassed.[190] And fingerprint technology had significant weaknesses: some ten percent of the population had worn, cut, or unrecognizable prints.[191] The solution was to move beyond a unimodal biometric identifier (e.g., fingerprints), and towards multimodal biometric identifiers, such as FRT, and voice, iris recognition technologies.

186. *State & County QuickFacts: USA*, U.S. CENSUS BUREAU, http://quickfacts.census.gov/qfd/states/00000.html (last visited Nov. 2, 2012).

187. GOV'T ACCOUNTABILITY OFFICE, GAO-11-276, DEFENSE BIOMETRICS: DOD CAN BETTER CONFORM TO STANDARDS AND SHARE BIOMETRIC INFORMATION WITH FEDERAL AGENCIES 12 (2011), *available at* http://www.gao.gov/new.items/d11276.pdf.

188. *See* SEARCH ANNIVERSARY, *supra* note 177.

189. *Id.* at 8.

190. *Id.*

191. *Multimodal Biometrics*, BIOMETRICNEWSPORTAL.COM, http://www.biometricnewsportal.com/multimodal-biometrics.asp (last visited Nov. 2, 2012).

The gains from such an approach could be substantial: biometric data could be used to obtain new information, such as tying individuals to places and activities, targeting specific individuals, and revealing movement patterns.[192] The Bureau illustrated the point by noting the potential use of these technologies to scan individuals at political rallies, connecting persons in attendance to two or more events.[193] By deploying enhanced remote capabilities, the Bureau could not just engage in investigations of individuals suspected of criminal or other activity, but, together with closer ties with the Department of Defense and the Department of State, it could perform an intelligence-gathering function. In 2009, for example, the FBI's Criminal Justice Information Services (CJIS) explained that "[r]apid DNA processing technology" would help to "provide on-location DNA results for federal, state, and local crime investigations, military, and the Intelligence community."[194] NGI would replace the IAFIS system, offering "state-of-the-art biometric identification services."[195] The project was expected to cost some $1 billion.[196]

It is important to underscore the extent to which NGI represents a change in how the Bureau uses biometric technologies. NGI relies in part on remote biometric identification to support investigatory and intelligence-gathering functions and thus represents something different in kind from what has been used before.

NGI itself includes seven components. (See Figure 2). Each component is itself substantial and involves associating biometric information with biographic data, providing a fuller picture of the target in question and allowing for the generation of new knowledge about individuals.

The first NGI program, Advanced Fingerprint Identification Technology (AFIT),[197] replaced IAFIS with an automated facial recognition search capability, as well as a broader range of data (such as name, address, social security number, telephone number, e-mail address, photograph, or other unique

192. SEARCH ANNIVERSARY, *supra* note 177, at 6.

193. *See id.* at 5–7.

194. *Id.* at 9.

195. *Id.* at 10.

196. Sternstein, *supra* note 137.

197. CRIMINAL JUSTICE INFO. SERVS. DIV., FED. BUREAU OF INVESTIGATION, CJIS ANNUAL REPORT 18 (2011), *available at* http://www.fbi.gov/about-us/cjis/annual-report-2011/annual-report-2011.

identifying number, code, or characteristic) which, when combined, indirectly identify an individual (such as a combination of gender, race, birth date, geographic indicator, license number, vehicle identifier including license plate, and other descriptors).[198] Under the new program, information can be obtained from federal, state, or local government entities, commercial data aggregators, or other private actors.[199]

AFIT has been given a functionality that previously did not exist within IAFIS: rapid fingerprint search of what is called the Repository for Individuals of Special Concern. According to the FBI, this database will be populated by records of "Known and Suspected Terrorists" (echoing HSPD-24)[200] as well as "other persons of special interest."[201] The Bureau does not explain what is meant by "Suspected Terrorists," nor does it publicly define individuals of "special interest"—a seemingly unlimited category.[202] Both fingerprint and facial recognition capabilities are included.[203] Under development is the system's relationship to something called the International Terrorist File.[204]

198. *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS)*, *supra* note 18.

199. *Id.*

200. HSPD-24, *supra* note 106.

201. CRIM. JUST. INFO. SERVICES DIV., FED. BUREAU OF INVESTIGATION NEXT GENERATION IDENTIFICATION, (2009) [hereinafter NEXT GENERATION IDENTIFICATION, http://www.biometriccoe.gov/_doc/FBI_CJIS_0209_NGI_One Pager020409.pdf. A PIA released in July 2012 explains that its purpose is "to identify persons who present special risks to the public or law enforcement personnel or heightened investigative interest." *Privacy Impact Assessment, Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) Repository for Individuals of Special Concern (RISC)*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/foia/privacy-impact-assessments/iafis-ngi-risc (last visited Nov. 2, 2012), [hereinafter RISC PIA].

202. *See also* CRIMINAL JUSTICE INFO. SERVS. DIV., FED. BUREAU OF INVESTIGATION, TECHNICAL SPECIFICATIONS DOCUMENT FOR THE REPOSITORY FOR INDIVIDUALS OF SPECIAL CONCERN (RISC) PILOT PROJECT 9 (2010), *available at* https://www.fbibiospecs.org/docs/RISC_Pilot_Technical_Specifications_Document_3.0.pdf (declining to define the term "special concern" and instead simply stating that the aim of the RISC pilot is "to provide the capability to receive and store biographic and fingerprint information associated with individuals marked as special concern"). The PIA for the program specifically contemplates further expansion, to include categories such as missing persons or protection order subjects that have associated biometrics; in such a case, the PIA would be annotated to reflect further additions of categories of records. RISC PIA, *supra* note 201.

203. FED. BUREAU OF INVESTIGATION CRIMINAL JUSTICE INFO. SERVS. DIV., *supra* note 202, at 19–22.

204. *Id.* at 13, 25–26.

Domestic as well as foreign agencies provide names and information for the RISC database.[205] For the former, local law enforcement serves as the front line of intelligence collection efforts.[206] RISC essentially allows police officers to use mobile devices to obtain thousands of fingerprints to then run them against the database.[207] Within seconds, the officer will receive a response—and the agency which first entered the biometric information into the database will be informed of a hit.[208] Pilot state programs have been run by Ohio, Florida, Maryland, Georgia, and Texas.[209] *Government Computer News* reported that the system began operating in March 2011; by August 2011, it had begun supporting 18,000 law enforcement agencies.[210] In 2011, the Program Manager of the Information Sharing Environment reported to Congress that the database, comprised of "the worst of the worst," had expanded to include some 1.2 million fingerprint records.[211]

The second capability incorporated into NGI is what is called a "Rap Back Service."[212] This function provides for private and public employers to enroll employees in the program, at which point the FBI will collect the employees' biometric data.[213] The gathering of IBI is paired with RBI: employers will

205. *Id.* at 9.

206. RISC PIA, *supra* note 201 ("This information will have been collected and submitted to the FBI by federal, state, local, tribal and some foreign agencies and instrumentalities incident to their lawful mission.").

207. *Id.* ("The fingerprints will be captured by a mobile fingerprint device and transmitted wirelessly to the user agency's existing criminal justice infrastructure, then on to the RISC.").

208. *Id.*; *see also* Alice Lipowicz, *FBI Mobile Fingerprint System Puts Criminals at RISC*, GOV'T COMPUTER NEWS, Aug. 26, 2011, http://gcn.com/articles/2011/08/25/fbi-fingerprint-check-system-national-database-mobile.aspx.

209. INFO. SHARING ENV'T, ANNUAL REPORT TO THE CONGRESS 70 (2011), *available at* http://www.nctc.gov/itacg/docs/ISE-Annual-Report-to-Congress-2011.pdf; *see also* William M. Kalaf, Arizona Law Enforcement Biometrics Identification and Information Sharing Technology Framework 16 (Mar. 2010) (unpublished Master's thesis, Naval Postgraduate School), *available at* http://www.hsdl.org/?view&did=27191 (listing Ohio, Florida, Texas, and Minnesota as running RISC pilot programs).

210. Lipowicz, *supra* note 208.

211. INFO. SHARING ENV'T, *supra* note 209, at 70. By June 13, 2011, more than 75,000 total live queries had been submitted, yielding more than 1,300 hits. *Id.*

212. Ellen Nakashima, *FBI Prepares Vast Database of Biometrics*, WASH. POST, Dec. 22, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/12/21/AR2007122102544.html (providing a brief overview of the Rap Bank Service).

213. *Id.* ("[E]mployers could ask the FBI to keep employees' fingerprints in

subsequently be notified by the Bureau "of criminal and, in limited cases, civil activity of enrolled individuals that occurs after the initial processing and retention of criminal or civil fingerprint transactions."[214] Notably, this includes both criminal and civil activities—activities that could relate to otherwise protected First Amendment activities. It essentially expands the biometric data collected by the FBI and creates a reporting-back mechanism that may take account of everything from attendance at political rallies, to parking violations, to formal charges related to serious crimes.[215]

The third function of NGI relates to Disposition Reporting Improvements (DRI). NGI DRI are designed to provide a more complete criminal history database. This system appears to incorporate the Interstate Identification Index into the FBI Identification Records.[216]

A fourth NGI initiative creates a new National Palm Print System, which complements the fingerprint system by populating a parallel database with known and unknown palm prints.[217] Criminal and noncriminal justice agencies across the country will be able to search the database, as well as use latent palm prints to search the data repository.[218]

An Enhanced IAFIS Repository (EIR) provides the fifth aspect of NGI. This capability will create compatibility between existing civil and criminal data bases, and ensure that the Bu-

the database, subject to state privacy laws, so that if [sic] employees are ever arrested or charged with a crime, the employers would be notified.").

214. *5 Things You Should Know About the FBI's Massive New Biometric Database (Alternet)*, UNCOVER THE TRUTH (2012), http://uncoverthetruth.org/category/foia-documents/page/2 (quoting FBI document that describes features of the Rap Back Service).

215. *Id.* No PIA is yet available from the FBI in regard to the Rap Back Service.

216. U.S. DEPT. OF JUSTICE, THE ATTORNEY GENERAL'S REPORT ON CRIMINAL HISTORY BACKGROUND CHECKS 3 (2006), *available at* http://www.justice.gov/olp/ag_bgchecks_report.pdf ("The Federal Bureau of Investigation (FBI) maintains a criminal history record repository, known as the Interstate Identification Index (III or 'Triple I') system, that contains records from all states and territories, as well as from federal and international criminal justice agencies.").

217. *Next Generation Identification*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi (last visited Nov. 2, 2012).

218. *Id.*

reau can conduct what is called single identity management.[219] According to the Bureau, "[t]he EIR will support the search and retrieval services for new biometric modalities, to include the iris, and provide administrative functions for special population files."[220] Precisely what these functions are, or who constitute the special population, is not spelled out.[221]

The sixth NGI program centers on iris recognition. This technology will allow the government to search a nationwide database of iris scans to quickly identify persons "of interest."[222] The FBI has made almost no information available about details of this program—such as the distance at which iris technologies could work (although private industry reports developing iris scans at a distance with the assistance of government grants, even as commercial systems are now available that claim accuracy two or more meters from the target).[223] Nor is there any information about how this database will be populated, by whom, or how the information is to be kept, used, and shared. No PIAs have yet issued.

The seventh component, and one of the most important aspects of NGI for remote biometric identification, is the Interstate Photo System (IPS). This project draws heavily on FRT

219. NEXT GENERATION IDENTIFICATION, *supra* note 201 ("The EIR capability will allow compatibility between existing civil and criminal repositories as well as new repositories by providing single identity management.").

220. *Id.*

221. *Id.* (mentioning only Rap Back Service features).

222. *See* Matt Bewig, *FBI Prepares Billion-Dollar Iris Recognition Database*, ALLGOV (July 8, 2012), http://www.allgov.com/news/where-is-the-money-going/fbi-prepares-billion-dollar-iris-recognition-database?news=844739 ("[T]he FBI plans to test a nationwide database for searching iris scans to more quickly identify persons 'of interest' to the government.").

223. *See, e.g.*, Charlie Leocha, *New Iris Scanning System Scans 30 Passengers per Minute at a Distance*, CONSUMER TRAVELER (Apr. 26, 2010), http://www.consumertraveler.com/today/new-iris-scanning-system-scans-30-passengers-per-minute-at-a-distance (reporting that Sarnoff Corporation won "Best New Product Award and Best Biometrics and Identity Solution at the Security Industry Association New Product Showcase" for a system allowing remote iris scanning and explaining that "[t]his technology was developed under a government grant to create an iris recognition at a distance solution"); Tom Olzak, *The Future of Iris Scanning*, TECH REPUBLIC (July 6, 2010), http://www.techrepublic.com/blog/security/the-future-of-iris-scanning/3978 (citing Sarnoff's Iris On The Move (IOM) scanning system); *see also Registered Traveler Programs*, AOPTIX TECH., http://www.aoptix.com/identity-solutions/high-throughput/applications/registered-traveler-programs (last visited Nov. 2, 2012) (technology allows remote iris scans at a distance of two meters); HUMAN RECOGNITION SYS., http://www.hrsid.com/mflow (last visited Nov. 2, 2012) (technology allowing for passage through airports).

and data mining technologies—and the database on which it is built is rapidly growing.[224] As of 2009, IAFIS included more than 6.75 million photos.[225] By February 2012, this number had increased to more than 114.5 million photos.[226] This number is expected to increase substantially.[227]

Three factors (in addition to the sheer power of new technologies) are influencing the rapid expansion of this database. First, NGI IPS incorporates media obtained not just from law enforcement, but from private businesses, social networking sites, government agencies, and foreign and international entities, as well as individuals such as acquaintances, friends, and family members.[228] This means that data derives from more sources. Second, as a structural matter, many of the limits previously placed on the collection of photos have been eliminated.[229] There are fewer restrictions, for instance, on the number of photos that can be submitted, new provisions to allow for bulk transfers of photos, new technologies to provide for the incorporation of video surveillance feeds, and new ways to submit descriptions of personal features.[230] These enhancements, "al-

224. NEXT GENERATION IDENTIFICATION, *supra* note 184, at 19–20.

225. *Id.* at 5.

226. *Integrated Automated Fingerprint Identification System: Fact Sheet*, FED. BUREAU OF INVESTIGATION (Oct. 16, 2012), http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis_facts.

227. *See* NEXT GENERATION IDENTIFICATION, *supra* note 184, at 19–20, 30 (noting the new functionality of allowing for the bulk submission of photos and the aim of providing law enforcement with "a large scale facial recognition investigative tool").

228. The program's PIA explains that images will be obtained not just from law enforcement, but "from other sources (such as security cameras, friends, family) . . . . Authorized noncriminal justice agencies and entities will be permitted to submit civil photographs along with civil fingerprint submissions that were collected for noncriminal purposes. . . . Selected foreign and international agencies may similarly contribute criminal and civil photo submissions for retention in the NGI IPS." *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS)*, *supra* note 18, at § 1.2.1.

229. *Id.* §§ 1.6, 1.7, 2.3.

230. *See id.*; Stan Shyshkin, *The FBI's Biometric Recognition System Is Now a Reality*, BRICKHOUSE SECURITY (Oct. 12, 2011), http://blog.brickhousesecurity.com/2011/10/12/fbis-biometric-recognition-system. Specifically, enhancements include eliminating the restriction of ten photo sets per FBI record, allowing the submission of photos with all arrests supported by fingerprints and/or an FBI number/Universal Control Number (FNU/UCN), allowing bulk submission of photos linked with FNUs/UCNs, allowing submission of photos with civil types of transactions, allowing submission of photos other than facial, allowing investigative search of photos using biographical criteria, and providing an automated facial recognition search capability. *Pri-*

low more photos to be retained in the system[,] . . . allow searches using better physical descriptor algorithms and facial recognition technology, and . . . allow more direct retrieval of such photos by an authorized requestor."[231] Third, a broader range of information qualifies for inclusion. That is, the media initially submitted may not, at first, provide identification related to arrest or conviction—instead, it may be merely contextual data that can subsequently be mined for information.[232] The FBI explains:

> IAFIS currently can collect and retain latent fingerprints from as yet unidentified individuals associated with criminal activity or otherwise having a lawful investigative or national security interest (such as fingerprints lifted from a crime scene). NGI IPS will also add an analogous functionality to collect and retain other images (such as those obtained from crime scene security cameras). Even though such images may not initially suffice to identify the particular individual in question, the images may later serve to directly or indirectly identify the individual if supplemental identifying information is located.[233]

The functionality of IPS is broader than the specific example provided. It is not just security cameras at the scene of a crime contributing data, but information from civil agencies, social network sites, private entities, and the like. By populating the database in this manner, photos and footage that may not initially be linked to a particular individual may be maintained in a common photo file and later associated with an identified individual.[234] Subjects included in the database may be unaware that their image or actions were even recorded—much less then fed into the system.[235]

vacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS), *supra* note 18, at §§ 1.4, 1.7; *see also* Shyshkin, *supra*.

231. *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS)*, *supra* note 18.

232. *See id.*

233. *Id.* The system is not to be used for data mining to discern, "previously unknown or predictive patterns," but rather in relation to specific queries. *Id.*

234. *See* NEXT GENERATION IDENTIFICATION, *supra* note 184, at 19; *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS)*, *supra* note 18 ("Photos which upon submission cannot be sufficiently linked to a particular identity will be maintained in a common photo file, though they may later be associated with an identified individual's file if determined to be related.").

235. *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS)*, *supra* note 18 (noting that individuals may not be provided direct notice of collection of information incident to law enforcement response" to their possible involvement in criminal activities).

The FBI acknowledges that biometric technology, since its emergence in the 1960s, had been plagued by inaccuracy and technological challenges.[236] Recent studies by the National Research Council of the National Academies underscore this concern: "[N]o biometric characteristic, including DNA, is known to be capable of reliably correct individualization over the size of the world's population."[237] Combined with problems due to environmental factors, injury, illness, data integrity, image quality, and the like, systems relying on biometric identification are bound to exhibit a high rate of error.[238] The question, however, is not whether the Bureau will make broader use of biometrics, but how soon it can be deployed.[239] The FBI is planning for a nationwide release of the system to all criminal justice professionals in 2014.[240] The system is being developed by private contractors Lockheed Martin and Security Solutions.[241]

236. *See infra* notes 822–32.

237. COMPUTER SCI. & TELECOMMS. BD., BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES 30 (Joseph N. Pato & Lynette I. Millett, eds., National Research Council of the National Academies 2010), *available at* http://www.nap.edu/openbook.php?record_id=12720&page=R1.

238. *Id.* at 1–14.

239. *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS)*, *supra* note 18 ("The FBI thus considers that incorporation of this technology into IAFIS promises to provide substantial benefits to law enforcement and national security, but that at the same time any facial recognition capability must be carefully assessed and tested prior to implementation to ensure that [it] is sufficiently reliable to provide the desired benefits and minimize erroneous identifications."). NGI is being implemented in phases. In January 2012, the system will be used in Michigan, Washington, Florida, and North Carolina. Shyshkin, *supra* note 230; Sternstein, *supra* note 137.

240. Shyshkin, *supra* note 230.

241. D.J. Pangburn, *FBI Introduces Next Generation Facial Recognition Technology*, DEATH & TAXES, Oct. 20, 2011, http://www.deathandtaxesmag.com/152857/fbi-introduces-next-generation-facial-recognition-technology; Sternstein, *supra* note 137. Note that privacy advocates have come out strongly against NGI. The Electronic Frontier Foundation argues that it "will result in a massive expansion of government data collection for both criminal and noncriminal purposes." Jennifer Lynch, *FBI Ramps Up Next Generation ID Roll-Out—Will You End Up in the Database?*, ELECT. FRONTIER FOUND. (Oct. 19, 2011), https://www.eff.org/deeplinks/2011/10/fbi-ramps-its-next-generation-identification-roll-out-winter-will-your-image-end. Concern turns in part on the fact that individuals engaged in a range of otherwise constitutionally-protected activities could be swept up into the database. Pangburn, *supra* note 241. A staff attorney with the Center for Constitutional Rights points out that "'[t]he federal government is using local cops to create a massive surveillance system.'" Kerry McQueeney, *Face Recognition Software to Be Launched by FBI to Help Police Catch Wanted Criminals*, DAILY MAILONLINE (Oct. 8, 2011, 8:47 AM), http://www.dailymail.co.uk/news/article-2046780/Face-recognition-soft

NGI is not the Bureau's only biometric initiative. The FBI's Biometric Center of Excellence (created post-9/11 and housed at the Bureau) has various other projects underway. Like DHS and the State Department, DOJ is emphasizing the importance of information sharing.[242] The FBI, for instance, collaborated on the Action Plan implementing HSPD-24, which formalized the sharing of this information with federal, state, and local entities.[243] Nevertheless, NGI presents perhaps the clearest example of how technologies otherwise employed for immediate biometric identification purposes are now transforming into remote biometric identification systems.

4. Military Applications

The use of biometrics has quickly moved beyond civilian applications like border security, authentication, and law enforcement, to the military domain. Even within the military, the technologies have evolved to impact a broad range of DoD's mission activities.[244] It involves not just what DoD refers to as "friendly biometrics" (e.g., identification of soldiers, contractors, and other personnel), but also matching biometric data found at the scene of attacks, engaging in counter-IED efforts, identifying detainees, providing further information about individuals held in custody, confirming targets for both manned and unmanned attacks, and confirming the identity of those killed.[245] Military applications represent one of the most significant leaps forward in biometric technologies, with developments ranging from the deployment of handheld systems to the use of widespread biometric enrollment for census taking.[246] Many of these initiatives bridge the gap between IBI and RBI, suggesting a shift to the latter sphere.

ware-launched-FBI-help-police-catch-wanted-criminals.html#ixzz1dMSAFcUt. The Cato Institute further notes that having mug shots from bookings means that even nonconvicted people would be in the system. Sternstein, *supra* note 137.

242. SEARCH ANNIVERSARY, *supra* note 177, at 6.

243. *Id.*

244. *See* BIOMETRICS TASK FORCE, *supra* note 25.

245. BIOMETRICS TASK FORCE, DEP'T OF DEF., ANNUAL REPORT FY09, at 14, 27, 33 (2009), *available at* http://www.fas.org/man/eprint/biometric09.pdf.

246. Thom Shanker, *To Track Militants, U.S. Has System That Never Forgets a Face*, N.Y. TIMES, July 13, 2011, at A1, *available at* http://www.nytimes.com/2011/07/14/world/asia/14identity.html?pagewanted=all ("[T]he government can scan through millions of digital files in a matter of seconds, even at remote checkpoints, using hand-held devices distributed widely across the security forces.").

In 2004, DoD's ABIS, designed to work with the FBI's IAFIS, became operational.[247] (Note that DoD and the State Department operate separate ABIS systems.) This system was the first multimodal fusion database in existence at the federal level. By 2009, DoD's ABIS had evolved into the Next Generation ABIS (NG-ABIS), a system that now combines fingerprint, palm print, FRT, and iris analysis with biographic and encounter data.[248] DoD's standards have correspondingly evolved away from individual transactions and, instead, towards application profiles.[249]

ABIS encompasses an electronic database and a set of software applications designed to support the storage, retrieval, and search of data collected from "persons of national security interest."[250] Exactly what this means, or what limits might apply, is not entirely clear. At a minimum, information from individuals seeking access to U.S. installations and bases is fed into the repository, as is data obtained by soldiers in the field.[251] Handheld devices collect fingerprint, face, and iris scans.[252] DoD's Biometrics Fusion Center, upon receiving transmitted images from the field, conducts a search of "all appropriate domestic and international databases" and forwards match results to those inquiring as well as to the intelligence community.[253] Such repositories include, inter alia, IAFIS and IDENT.[254]

247. BIOMETRICS IN GOVERNMENT POST-9/11, *supra* note 38, at 10. The two systems share a common interface; additionally, DoD's Electronic Biometric Transmission Specifications are based on the FBI and ANSI standards. BIOMETRICS TASK FORCE, *supra* note 25, at 1.

248. BIOMETRICS TASK FORCE, *supra* note 25, at 1, 6.

249. *Id.* at 6.

250. *Id.* at 1.

251. *See* Memorandum from Gordon R. England, Acting Deputy Sec'y of Def. to Sec'ys of the Military Dep'ts, Chairman of the Joint Chiefs of Staff, Under Sec'ys of Def., Commanders of the Combatant Commands & Dirs. of the Def. Agencies 2 (July 15, 2005) [hereinafter DoD Memorandum], *available at* http://www.dtic.mil/whs/directives/corres/pdf/dsd050715iraq.pdf.

252. *See, e.g.*, BOB CARTER, LOCKHEED MARTIN, DOD BIOMETRICS, DOD ABIS: QUALITY EVALUATION OF OPERATIONAL MULTI-MODAL BIOMETRIC DATA 2 (2006), *available at* http://biometrics.nist.gov/cs_links/quality/workshopI/proc/carter_dod_abis_multi-modal_quality_for_publication.pdf. Note that the collection of this data is not without difficulty: cluttered backgrounds, legacy data, non-frontal poses, inconsistent lighting, multiple heads, and low resolution prove to bedevil face data quality for efficient application of FRT. *Id.* at 13.

253. DoD Memorandum, *supra* note 251, at 2.

254. *See infra* Part I.B.5.

In addition to the database itself, DoD has now created a Biometrically Enabled Watch List (BEWL). The so-called BEWL Tiger Team was created in 2010 to consider BEWL stakeholders and the appropriate standards.[255] The creation of such a list echoes that established by DHS.[256]

In 2006, DoD established Defense Biometrics as its office for biometric enterprise management.[257] The Biometrics Task Force, in turn, became the executing agency.[258] At the same time, the Defense Science Board launched a Task Force to study the use of biometrics in DoD.[259] Agencies, working through the National Science and Technology Council (NSTC) and the National Security Council, began to design government-wide biometric systems that would be operable between agencies.[260] By 2006 DoD had published a Biometrics Concept of Operations. Various Combatant Command (COCOM) strategies subsequently evolved, based on this document.[261] Military branches have further integrated biometrics into their planning and strategy documents.[262]

Military applications of biometric technologies continue to evolve. Confirmation of both Osama bin Laden and Muammar Gaddafi's deaths, for instance, came through the use of facial recognition technology.[263] Increasing interest has been shown in DoD's domestic role along the U.S. border.[264] In September

255. DOD BIOMETRICS COLLABORATION FORUM, *supra* note 26, at 22–23.

256. *Id.* at 15 (noting that technologies "[a]llow[] matches against watchlists, DoD, FBI, and DHS biometric databases").

257. *See Biometrics: A Decade of Progress Since 9/11*, *supra* note 105.

258. BIOMETRICS IN GOVERNMENT POST-9/11, *supra* note 38, at 10.

259. *Id.*

260. *Id.*

261. DOD BIOMETRICS COLLABORATION FORUM, *supra* note 26, at 27-28 (describing and identifying strategies involving COCOMs).

262. The USMC, for instance, has adopted an Identity Operations (IdOps) Strategy 2020, which is focused on coordinating planning and resourcing activities aimed at institutionalizing and integrating IdOps within the USMC. It includes USMC Biometrics and Forensics strategies. DOD BIOMETRICS COLLABORATION FORUM, *supra* note 26, at 11–13, 16, 20.

263. Jake Tapper, *Facial Recognition Technology Used to Confirm Gadhafi's Death*, ABC NEWS, Oct. 20, 2011, http://abcnews.go.com/blogs/politics/2011/10/facial-recognition-technology-used-to-confirm-gadhafis-death.

264. The DoD biometrics community (Biometrics Identity Management Agency, Office of the Under Secretary for Policy, and Special Operations Command) has partnered with DHS and CBP to consider how biometrics could be used along the borders. DOD BIOMETRICS COLLABORATION FORUM, *supra* note 26, at 10-11 (di scussing the poor oversight and implementation of the civilian project to secure the U.S. border and noting, "[t]he DoD has broad ex-

2011, reports surfaced that DoD, in conjunction with Georgia Tech Research Institute, had begun testing autonomous aerial drones that combined FRT with targeting abilities.[265]

Considerable resources are being spent on biometrics, reflecting the fact that myriad military biometric applications present themselves. Between 2007 and 2015, DoD plans to spend $3.5 billion on biometrics.[266] Institutional arrangements are becoming formalized: in 2010, the Biometrics Task Force transitioned to the Biometrics Identity Management Agency, a centralized DoD hub for biometric data management.[267] The Secretary of the Army now serves as DoD Executive Agent for biometrics.[268]

5. Interoperability

In addition to the individual biometric programs and databases that integrate RBI technologies are renewed efforts to ensure cross-agency access to information. Both the executive and legislative branches emphasize the importance of such interoperability. This is significant to the extent that it suggests movement towards a sort of supra-national RBI system. Such interoperability, moreover, is fueled by multiple sources of funding, providing greater resources to generate growth. Simultaneously, it reflects diffuse accountability. That is to say, no one committee is tasked with considering the implications of the overall system. A handful of examples illustrate how efforts to encourage inter-agency sharing of data are expanding federal capabilities with regard to RBI.

In 2003, NSTC chartered a subcommittee on biometrics with the explicit aim of coordinating the multitude of initiatives launched across the federal government.[269] Three years later, government agencies, "working through the NSTC, [began] the process of designing government-wide biometric system in-

perience in using biometrics and other sensors to contribute to secure borders, Ports of Entry and cities").

265. John P. Mello, Jr., *Facial Recognition: Facebook Photo Matching Just the Start*, PC WORLD, Sept. 21, 2011, http://www.pcworld.com/article/240363/facial-recognition-facebook-photo-matching-just-the-start.html.

266. GOV'T ACCOUNTABILITY OFFICE, GAO-11-276, DEFENSE BIOMETRICS: DOD CAN BETTER CONFORM TO STANDARDS AND SHARE BIOMETRIC INFORMATION WITH FEDERAL AGENCIES (2011) [hereinafter GAO-11-276], *available at* http://www.gao.gov/assets/320/317368.

267. *Id.* at 4–5.

268. DoD Memorandum, *supra* note 251, at 3.

269. BIOMETRICS IN GOVERNMENT POST-9/11, *supra* note 38, at 9.

teroperability."[270] The following year, agencies, working with both the NSTC and the National Counterterrorism Center, initiated a project to improve biometric coordination with regard to known and suspected terrorists.[271] This was followed in June 2008 with HSPD-24, which underscored the importance of adopting mutually compatible methods and procedures to collect, store, use, analyze, and share biometric information across federal agencies.[272] The directive sought to ensure that the objectives described in previous executive orders and directives could be accomplished.[273] The policy henceforward would be for agencies to use integrated processes and interoperable systems to "make available to other agencies all biometric and associated biographic and contextual information associated with persons for whom there is an articulable and reasonable basis for suspicion that they pose a threat to national security."[274] The Secretaries of State, Defense, and Homeland Security, the Attorney General, the Director of National Intelligence, and the heads of other agencies would henceforward be required to "[m]aintain and enhance interoperability among . . . biometric and associated biographic systems[] by utilizing common information technology and data standards, protocols, and interfaces."[275] To assist in interoperability for the new and emerging biometric fields—and particularly for facial recognition—new standards were issued.[276]

270. *Id.* at 10.

271. *Id.*

272. HSPD-24, *supra* note 106, at 788; *see also* BIOMETRICS IN GOVERNMENT POST-9/11, *supra* note 38, at 11.

273. HSPD-24, *supra* note 106, at 788–89.

274. *Id.* at 790.

275. *Id.*

276. *See* BIOMETRICS IN GOVERNMENT POST-9/11, *supra* note 38, at 10–11. For examples of such standards, see SUBCOMM. ON BIOMETRICS, NAT'L SCI. & TECH. COUNCIL, BIOMETRICS STANDARDS 2–3 (2006), *available at* http://www.biometrics.gov/Documents/biostandards.pdf; NAT'L INST. OF STANDARDS & TECH., INFORMATION TECHNOLOGY: AMERICAN NATIONAL STANDARDS FOR INFORMATION SYSTEMS—DATA FORMAT FOR THE INTERCHANGE OF FINGERPRINT FACIAL, & OTHER BIOMETRIC INFORMATION—PART 1, at 1 (2007), *available at* http://www.nist.gov/itl/ansi/upload/Approved-Std-20070427-2.pdf (adopted to include data fields to support best practices application levels for the capture of facial images and a new record type for iris data); SUBCOMM. ON BIOMETRICS & IDENTITY MGMT., NAT'L SCI. & TECH. COUNCIL, NSTC POLICY FOR ENABLING THE DEVELOPMENT, ADOPTION AND USE OF BIOMETRIC STANDARDS 3 (2007), *available* at http://www.biometrics.gov/Standards/NSTC_Policy_Bio_Standards.pdf; NAT'L INST. OF STANDARDS & TECH., INFORMATION TECHNOLOGY: AMERICAN NATIONAL STANDARD FOR INFORMATION SYSTEMS—DATA FORMAT FOR THE INTERCHANGE OF FINGERPRINT FACIAL, & OTHER BIOMETRIC

Congress also took steps that underscored the importance of interoperability: in 2004, for instance, the Intelligence Reform and Terrorism Prevention Act required the President to establish an Information Sharing Environment "for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties."[277] It established a Program Manager for the Information Sharing Environment (PM-ISE) who, in consultation with the interagency Information Sharing Council, is responsible for overseeing the implementation and management of the Information Sharing Environment (ISE).[278] The PM-ISE assisted the President in developing and submitting an ISE Implementation Plan to Congress.[279] This plan focused on five areas (intelligence, law enforcement, defense, homeland security, and foreign affairs) and called for these communities to be granted expedited access to protected terrorism information.[280] "We envision a future," the Plan, issued in 2006, stated, "that represents a *trusted partnership among all levels of government in the United States, the private sector, and our foreign partners, to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism against the territory, people, and interests of the United States of America*."[281] More directly, the plan specified the importance of ensuring access to personally identifiable information (fingerprints, photographs, and biometric indicators) for information discovery and search functions across federal agencies.[282]

Not only did Congress pass statutes that reinforced the importance of sharing information across federal agencies,[283]

INFORMATION—PART 2: XML VERSION viii (2008), *available at* http://www.nist.gov/itl/ansi/upload/Approved-XML-Std-20080828.pdf (adopted to support modern data exchange protocols such as web services).

277. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1016, 118 Stat. 3638, 3664–70 (to be codified at 6 U.S.C. § 485).

278. *Id.*

279. *Id.*

280. INFO. SHARING ENV'T, IMPLEMENTATION PLAN xiii (2006), *available at* http://www.ise.gov/sites/default/files/ise-impplan-200611_0.pdf.

281. *Id.* (emphasis in original).

282. *Id.* at 45.

283. *See, e.g.*, Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No 108-458, § 7402, 118 Stat. 3638, 3850 (increasing the authority of the Department of Homeland Security to utilize private sector resources that would assist in preventing, or responding to, terrorist acts); Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. No. 107-173, § 201(a), 116 Stat. 543, 547 ("Federal law enforcement agencies and the intelligence community shall . . . share any information . . . relevant to the admissibility

but it repeatedly drew on its public hearings and oversight mechanisms to press the executive on the failure of specific programs to further integrate.[284]

With such strong messaging coming both from the White House and Congress, agencies have worked to ensure the interoperability of their systems. It is not that there was no previous effort to do this: more than one year before the 9/11 attacks, for instance, DOJ developed an initial implementation plan for interoperability of INS's IDENT and the FBI's IAFIS.[285] But it was not until after the attacks that INS (and its successor, DHS), together with DOJ and DOS, made substantial progress.[286]

The first step in developing interoperability between IAFIS and IDENT consisted of deploying approximately 150 IDENT and IAFIS workstations to border locations, enabling simultaneous fingerprint checks.[287] Following this, in 2004, updated hardware and software enabled integration of the two databases into a single workstation.[288] The FBI then reverse-engineered IAFIS with the capability to store biographic and biometric information from the IDENT apprehension database—at the same time allowing other federal, state, and local enforcement agencies to submit fingerprints to IDENT for verification.[289] Integration of the systems continued. These initiatives prompted DHS to issue a PIA for IDENT/IAFIS Interop-

and deportability of aliens . . . ."); Homeland Security Act of 2002, Pub. L. No. 107-296, § 102(a),(b)(3), 116 Stat. 2135, 2142–43 (creating the position of Secretary of Homeland Security and requiring the Secretary to "take reasonable steps to ensure that information systems and databases of the Department [of Homeland Security] are compatible with each other and with appropriate databases of other [federal] Departments"); USA PATRIOT Act, Pub. L. No. 107-56, § 701, 115 Stat. 272, 374 (2001) (authorizing the establishment of enhanced information-sharing systems between federal, state, and local law enforcement agencies).

284. *See, e.g.*, H.R. REP. NO. 108-792, at 714 (2004) (Conf. Rep.) (supporting the coordination of law enforcement agencies and allocating funds to various coordination programs); H.R. REP. NO. 108-280, at 47 (2003) (Conf. Rep.) (requesting a report from the Department of Homeland Security detailing its prior efforts to coordinate and share information with other law enforcement agencies).

285. *See* DEP'T OF HOMELAND SEC., IDENT/IAFIS INTEROPERABILITY 2 (2005), *available at* http://www.dhs.gov/xlibrary/assets/foia/US-VISIT_IDENT-IAFISReport.pdf.

286. *Id.* at 2–3 (outlining the progress of IDENT/IAFIS interoperability after 9/11).

287. *Id.*

288. *Id.* at 3.

289. *Id.*

erability.[290] The Department envisioned a phased approach, in which federal, state, and local entities would eventually be brought into the information sharing environment.[291] By 2008, DOS had begun submitting all ten-print checks against IAFIS, using IDENT/IAFIS interoperability.[292] That same year DHS, DOS and the FBI signed a Memorandum of Understanding (MOU), as IDENT and IAFIS became fully interoperable.[293] The following year a similar MOU between DoD and the FBI was signed, as the Bureau began research on the enhanced capability IAFIS/Next Generation Identification.[294] In 2005, efforts began to integrate US-VISIT into the IDENT/IAFIS environment.[295] In 2006, DHS and the FBI adopted an Interim Data Sharing Model (iDSM) to provide for interoperability.[296]

Similar initiatives have now begun to mark DoD's relationship with DHS with regard to ABIS and IDENT. In 2011, for instance, DoD and DHS signed an MOU to establish a policy framework for moving forward with interoperability, leading to direct connectivity between the two databases.[297]

DoD's relationship with DOJ and the FBI is significantly more developed—at least with regard to the interoperability of ABIS and IAFIS. From the beginning, ABIS was designed to be interoperable with the FBI's IAFIS. In 2005, DoD's ABIS and the FBI's IAFIS became fully interoperable.[298] This paved the way for the military to begin exchanging latent prints (e.g., from improvised explosive devices found in the field) with IAFIS in 2007.[299] These two systems have continued to evolve

290. *See generally* DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE INTERIM DATA SHARING MODEL (IDSM) FOR THE AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (IDENT)/INTEGRATED AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM (IAFIS) INTEROPERABILITY PROJECT (2006), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_idsm.pdf.

291. *Id.* at 2–3, 8–9.

292. CRIMINAL JUSTICE INFO. SERVS. DIV. INTEROPERABILITY INITIATIVES UNIT, BIOMETRIC INTEROPERABILITY 9 (2011) [hereinafter BIOMETRIC INTEROPERABILITY], *available at* https://www.fbibiospecs.org/FacialRecogForum/Forum2/_Uploads/facial%20recog%20forum%20110211_1.pdf.

293. *See id.* at 4, 9.

294. *See id.* at 4.

295. *See id.* at 12.

296. *See id.* at 9.

297. *See id.* at 15.

298. *Id.* at 9.

299. *See* NAT'L SCI. & TECH. COUNCIL SUBCOMM. ON BIOMETRICS & IDENTITY MGMT., THE NATIONAL BIOMETRICS CHALLENGE 15–16 (2011), *available*

in tandem. This means that a soldier in the field can collect biometric information and, through the Biometric Fusion Center, run it against the FBI database. Any matches in the results are then transmitted back to the soldier and potentially distributed to intelligence agencies. The type of information may include not just biometric data, but past criminal record, the biometric subject's address, contact information, birth date, death date, place of death, citizenship, ethnicity, height, weight, blood type, marital status, group membership, encounter data, and other physical, social, and civic characteristics.[300] This information then becomes part of the military database.

The DoD-FBI relationship has continued to evolve. In 2010, for instance, groundbreaking occurred for the joint FBI/DoD Biometric Technology Center.[301] By March of 2011, DoD had adopted a standard for the collection of biometric information to facilitate sharing that information with other federal agencies.[302] The standards have been applied in some, but not all, of its collection devices.[303]

6. State and Local Government

Federal forays into this area are now extending to state and local government, raising parallel questions about statutory and constitutional framing, as well as concerns about the extent to which state and local initiatives are being folded into the federal framework.

Minnesota, for instance, runs CriMNet, which emphasizes biometric identification and information sharing.[304] The state uses mobile biometric identification devices for officers in the field, employs an automated fingerprint identification system during booking, and checks targets against the FBI's Reposito-

at http://www.biometrics.gov/Documents/BiometricsChallenge2011_protected.pdf.

300. BIOMETRICS TASK FORCE, *supra* note 25, at 16–24.

301. *See* Elizabeth Montalbano, *FBI Plans Biometrics Tech Center*, INFORMATIONWEEK GOV'T (Dec. 5, 2011, 3:40 PM), http://www.informationweek.com/government/information-management/fbi-plans-biometrics-tech-center/232200748.

302. *See* BIOMETRIC INTEROPERABILITY, *supra* note 292, at 2.

303. For instance, one handheld device, used primarily by the Army, is responsible for thirteen percent of the biometric records held by DoD—i.e., approximately 630,000 records. GAO-11-276, *supra* note 266. Because this device does not conform to the standards, the information contained cannot be checked against the FBI's approximately 94 million records. *Id.*

304. Kalaf, *supra* note 209, at 19, 25.

ry for Individuals of Special Concern.[305] Similarly, Wisconsin uses an Automated Fingerprint Identification System, as well as FAST ID, a mobile biometric identification system.[306]

Such systems can be found at the local level as well. Los Angeles County, California, for example, maintains two separate biometric identification systems.[307] The Los Angeles Regional Identification System supplies biometric information to law enforcement agencies and provides mobile identification capabilities to law enforcement officers.[308] Los Angeles County's system also has been integrated into the Los Angeles Police Department's centralized repository as well as the Regional Terrorism Information and Integration System.[309] In Florida, the Pinellas County Sheriff's Office has begun tapping into the state's Department of Highway Safety and Motor Vehicles' photo archives, allowing officers in the field, equipped with digital cameras, to quickly cross-check individuals detained against the photo bank.[310] The sheriff's office claims that between the launch of the program in 2004 and July 2011, some 700 arrests had been generated.[311]

The spread of biometric technologies to state and local government is driven in part by the availability of new technologies and by state initiatives. It has also been driven, however, by federal efforts to obtain more information. The Maricopa County (Arizona) Sheriff's Office (MCSO) explained to Congress how the local collection of information feeds directly into federal initiatives:

> As outlined in the Information Sharing Environment Implementation Plan state/local centers will become a part of the National Intelligence Program. As such if these centers provide direct support to ongoing Federal programs that require funding . . . then the Federal government should provide continued funding support. An example of this effort is the Maricopa County Sheriff's Office Facial Recognition Program. Working in conjunction with the U.S. Department of Justice the Facial Recognition Program has been provided with access to the

305. *Id.* at 25.

306. *Id.* at 21, 61.

307. *Id.* at 20.

308. *Id.* at 20, 48.

309. *Id.* at 49.

310. Glenn Bischoff, *Video: Facial Recognition Technology Nabs Criminals in Florida*, URGENT COMMC'NS. (Oct. 26, 2011, 5:42 PM), http://urgentcomm.com/mobile_data/news/pinellas-facial-recognition-20111026.

311. Emily Steel, *How a New Police Tool for Face Recognition Works*, WALL ST. J. BLOGS (July 13, 2011, 7:56 AM), http://blogs.wsj.com/digits/2011/07/13/how-a-new-police-tool-for-face-recognition-works.

> Federal Joint Automated Booking System and all of the Federal arrestee's photographs. In addition the MCSO is partnering with the Federal Bureau of Investigation to support their violent gang and criminal investigations through the use of the Facial Recognition Program. The MCSO is also working with agencies and fusion centers nationwide to establish a facial recognition network that will support criminal investigations and the recovery of missing and abducted children.[312]

Federal information, in turn, is then provided to local entities, further blurring the federalism divide. The Maricopa County Sheriff Department's Facial Recognition Unit, for instance, is building a database to match suspect photos with millions of images drawn from dozens of federal agencies.[313] State and local governments are thus both active participants in building federal biometric databases as well as consumers of federal initiatives.

The new technologies available to state and local government offer mobile biometric capture across a range of remote biometric identification technologies. For example, the Mobile Offender Recognition and Information System, known as MORIS, incorporates FRT, iris scans, and fingerprinting.[314] Police officers equipped with the device can take a picture of a person's face from a distance of two to five feet away, which is then analyzed according to 130 distinguishing points.[315] This

312. *The Way Forward with Fusion Centers: Challenges and Strategies for Change: Hearing Before the Subcomm. on Intelligence, Information Sharing, and Terrorism Risk Assessment of the H. Comm. on Homeland Security*, 110th Cong. 44 (2007) (statement of Norman Beasley, Coordinator for Counter Terrorism, Maricopa Cnty. Sheriff's Office) (examining federal challenges and strategies to improve homeland security and terrorist threat information sharing among federal, state, and local agencies through the establishment and utilization of fusion centers).

313. *Id.* at 50. Numerous agencies participate in the program "includ[ing]: FBI, ATF, U.S. Postal Inspection Service, TSA, ICE, U.S. Border Patrol, Arizona Department of Public Safety, Arizona National Guard, Arizona Department of Corrections, Arizona Department of Revenue, U.S. Department of State, Arizona Motor Vehicle Department, Arizona Attorney General's Office, Defense Intelligence Agency, Federal Air Marshal Service, Rocky Mountain Information Network, Phoenix Police Department, Phoenix Fire Department, Glendale Fire Department, Mesa Fire Department, Mesa Police Department, Glendale Police Department, Maricopa County Sheriff's Office, Air Force Office of Special Investigations, U.S. Secret Service, Internal Revenue Service, Maricopa County Attorney's Office, Scottsdale Police Department, Tempe Police Department, Arizona Department of Economic Security, Arizona Department of Liquor License and Control, and the U.S. Department of Homeland Security." *Id.*

314. Steel, *supra* note 311.

315. *Id.*

information can then be compared to existing databases.[316] In a similar manner, the officer can hold the device five to six inches from an individual's eye for a high-resolution image, or use a small metallic rectangle attached to the camera to scan the individual's fingerprints.[317] In 2010, police officers in Brockton, Massachusetts became the first police department to test the device, which by July 2011 was ready for deployment—with applications for iPhone and Android in the works.[318]

The funding for many state and local initiatives derives in part from federal agencies. Pilot programs, such as NGI, leverage investments in research and development to deploy new technologies. In some cases, the federal government continues to provide services to allow state and local actors to take full advantage of the technologies.[319] Money also has been made available for the purpose of helping local entities to develop their own systems. DOJ's Office of Community Oriented Policing Services, for instance, has issued grants to develop MORIS-type devices.[320]

In sum, what the state and local initiatives in this area demonstrate is the extent to which such technologies are becoming more common. They also show how federal initiatives in this area influence the collection of such information, and the way in which the line between law enforcement and national security is becoming increasingly blurred. The availability of resources is also tied to federal initiatives. Yet there are no federal statutes that address the difficult questions that accompany broader use of these technologies and the movement to remote biometric identification.

II. STATUTORY GAP

Congress has clearly and emphatically given federal agencies the authority to collect, analyze, and share personally identifiable information (PII). Such limits as have been introduced on the exercise of these powers, however—specifically in relation to (1) protecting PII; (2) obtaining information for use in criminal investigations; and (3) collecting foreign intelligence—

316. *Id.*

317. *Id.*

318. *Id.*

319. Heaton, *supra* note 29; Aliya Sternstein, *Facial Recognition Apps Spark Privacy Concerns in Congress*, NEXTGOV, Oct. 19, 2011, http://www.nextgov.com/nextgov/ng_20111019_1039.php.

320. Steel, *supra* note 311.

at best, only weakly apply, and at worst, fail altogether to address the types of technologies at work in remote biometric identification.

Within the first category, broad gaps in the 1974 Privacy Act, its amendments, and the 1990 Computer Act, paired with explicit exemptions in the Privacy Act and the 2002 E-Government Act, remove most biometric systems—much less RBI technologies such as facial recognition—from such restrictions.

The second category, dominated by Title III of the 1968 Omnibus Crime Control and Safe Streets Act and, subsequently, Title I of the 1986 Electronic Communications Privacy Act, says nothing about RBI generally, much less facial recognition technology. Moreover, while the latter two statutes address audio recording, *they do not address silent video recording*.

The third category, governed by the 1978 Foreign Intelligence Surveillance Act and its subsequent amendments, only addresses certain types of electronic communications and remains silent on the collection, and construction and use of databases populated with biometric and tracking technologies. Such rules as do apply to electronic surveillance would be almost impossible to translate to RBI systems. Targeting, the duration for which orders can be issued, minimization procedures, and special certification all depend upon distinguishing between U.S. persons and non-U.S. persons—a distinction almost meaningless in the context of RBI. The specificity otherwise required by statute, moreover, runs counter to the orientation of the technologies involved in this new and emerging area. This lack of statutory guidance thus drives us back upon constitutional analysis in considering the programs currently being developed by the federal government.

A. PERSONALLY IDENTIFIABLE INFORMATION

At the most general level, the Department of Justice,[321] Department of State,[322] Department of Homeland Security[323]

321. *See, e.g.*, 28 U.S.C. §§ 533, 534 (2006) (recognizing DOJ's authority to acquire, collect, classify, and preserve identification and other records, and to exchange them with other federal officials and state and local government entities); *see also* 50 U.S.C. § 404o (2006 & Supp. IV 2011) (supporting the DOJ's responsibility to disseminate terrorism information); Act of Oct. 25, 1972, Pub. L. No. 92-544, pmbl., 86 Stat. 1109, 1109 ("Making appropriations for the Departments of State, Justice, and Commerce, the Judiciary, and related agencies."). In addition, record-keeping authority has been delegated to the director of the FBI. 28 C.F.R. §§ 0.85, 20.1–20.3, 20.20–20.25, 20.30–20.38 (2012); *see*

also 8 U.S.C. § 1158(c) (2006) (immigration and asylum authorities); *id.* § 1225(b) (2006) (screening and asylum considerations), *subsection (b)(1)(D) invalidated by* United States v. Barajas-Alvarado, 655 F.3d 1077, 1087 (9th Cir. 2011); *id.* § 1357(a) (2006) (interrogation of aliens); *id.* § 1360(a) (2006) (establishment of a central index with the names of all aliens admitted or denied admission, their sponsors, and any other relevant information the Attorney General shall require); *id.* § 1365a(b) (2006) (integrated entry and exit system to be implemented by the Attorney General); *id.* § 1379(1) (2006) (directing the Attorney General and the Secretary of State to develop and certify a technology standard, including appropriate biometric identifier standards to verify the identity of persons applying for a U.S. visa or seeking to enter the United States); 44 U.S.C. §§ 3301–3312 (2006) (exchange of records); *see also* Hammons v. Scott, 423 F. Supp. 625, 628 (N.D. Cal. 1976) (stating that the FBI maintains arrest records).

322. *See* 8 U.S.C. § 1201 (2006) (giving the Department of State the authority to collect data in order to grant or deny visa applications); *see also id.* § 1324 (2006) (providing the authority for seizing property and evidence related to bringing in and harboring certain aliens); *id.* § 1365a (giving the Department of State the authority to maintain a database related to alien entry and exit); *id.* § 1379 (giving the Attorney General and the Secretary of State the authority to develop and certify a technology standard to verify the identity of aliens). More specific authority to collect personally identifiable information (PII) is given to the State Department with regard to ABIS, *see* U.S. DEP'T OF STATE, AUTOMATED BIOMETRIC IDENTIFICATION SYSTEM (ABIS) PRIVACY IMPACT ASSESSMENT 3 (2011), *available at* http://www.state.gov/documents/organization/109132.pdf (relying on the following as legal authority: "Immigration and Nationality Act (INA) 1952, 8 U.S.C. 1101, as amended[,] INA, 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)[,] 22 U.S.C 2651(a) (Organization of Department of State)[,] INA, 8 U.S.C. 1202(f) (Confidential Nature of Visa Records)[,] Immigration Act of 1990 (P.L. 101-649)[,] Illegal Immigration Reform and Immigration Responsibility Act (IIRIRA) of 1996[,] Omnibus Consolidated Appropriations Act, 1997 (P.L. 104-208)[,] Legal Immigration Family Equity 'LIFE' Act (Part of HR 5548, 2000)[,] USA PATRIOT Act of 2001 (HR 3162) (P. L. 107-56)[,] Enhanced Border Security and Visa Entry Reform Act of 2002 (HR 3525)[,] and Child Status Protection Act (HR 1209) 2002"), the Consular Consolidated Database, *see* CONSULAR CONSOLIDATED DATABASE (CCD) PIA, *supra* note 146, at 3–4 (relying on the following as legal authority: "8 U.S.C. 1401–1503 (2007) Acquisition and Loss of U.S. Citizenship or U.S. Nationality; Use of U.S. Passports)[,] 8 U.S.C. 1101–1503 (Immigration and Nationality Act of 1952, as amended)[,] 18 U.S.C. 911, 1001, 1541–1546 (2007) (Crimes and Criminal Procedure)[,] 22 U.S.C. 211a–218, 2651a, 2705[,] Executive Order 11295 (August 5, 1966)[,] 31 FR 10603 (Authority of the Secretary of State in granting and issuing U.S. passports)[,] 8 U.S.C. 1185 (Travel Control of Citizens)[,] 8 U.S.C. 1104 (Powers and Duties of the Secretary of State)[,] 22 U.S.C. 3904 (Functions of the Foreign Service, including protection of U.S. citizens in foreign countries under the Vienna Convention on Consular Relations and assistance to other agencies)[,] 22 U.S.C. 1731 (Protection of naturalized U.S. citizens in foreign countries)[,] 22 U.S.C. 2705 (Preparation of Consular Reports of Birth Abroad)[,] 8 U.S.C. 1501 (Adjudication of possible loss of nationality)[,] 22 U.S.C. 2671(b)(2)(B) (Repatriation loan for destitute U.S. Citizens abroad)[,] 22 U.S.C. 2670(j) (Provision of emergency medical, dietary and other assistance)[,] 22 U.S.C. 2151n–1 (Assistance to arrested citizens) (Repealed, but applicable to past records)[,] 42 U.S.C. 1973ff–1973ff–6 (Overseas absentee voting)[,] 42 U.S.C. 402 (Social

Security benefits payments)[,] Sec. 599C of Public Law 101-513, 104 Stat. 1979, as amended (Claims to benefits by virtue of hostage status)[,] 50 U.S.C. App. 453, 454, Presidential Proclamation No. 4771, July 2, 1980 as amended by Presidential Proclamation 7275, February 22, 2000 (Selective Service registration)[,] 22 U.S.C. 5501–5513 (Aviation disaster and security assistance abroad; mandatory availability of airline passengers manifest)[,] 22 U.S.C. 4196; (22 U.S.C. 4195, repealed, but applicable to past records) (Official notification of death of U.S. citizens in foreign countries; transmission of inventory of effects)[,] 22 U.S.C. 2715b (notification of next of kin of death of U.S. citizens in foreign countries)[,] 22 U.S.C. 4197 (Assistance with disposition of estates of U.S. citizens upon death in a foreign country)[,] 22 U.S.C. 4193, 4194[,] 22 U.S.C. 4205–4207[,] 46 U.S.C. 10318 (Merchant seamen protection and relief)[,] 22 U.S.C. 4193 (Receiving protests or declarations of U.S. citizen passengers, merchants in foreign ports)[,] 46 U.S.C. 10701–10705 (Responsibility for deceased seamen and their effects)[,] 22 U.S.C. 2715a (Responsibility to inform victims and their families regarding crimes against U.S. citizens abroad)[,] 22 U.S.C. 4215, 4221 (Administration of oaths, affidavits, and other notarial acts)[,] 28 U.S.C. 1740, 1741 (Authentication of documents)[,] 28 U.S.C. 1781–1783 (Judicial Assistance to U.S. and foreign courts and litigants)[,] 42 U.S.C. 14901–14954; Intercountry Adoption Act of 2000, (Assistance with Intercountry adoptions under the Hague Intercountry Adoption Convention, maintenance of related records)[,] 42 U.S.C. 11601–11610, International Child Abduction Remedies Act (Assistance to applicants in the location and return of children wrongfully removed or retained or for securing effective exercise of rights of access)[,] 22 U.S.C. 4802 (overseas evacuations)"), and the Identity Management System, *see* IDENTITY MANAGEMENT SYSTEM, PRIVACY IMPACT ASSESSMENT, *supra* note 175, at 3 (relying on the following as legal authority: "5 U.S.C. 301; Federal Information Security Management Act (FISMA)[,] National Defense Authorization Act, Act (Pub. L. 104-106, sec. 5113)[,] Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors, August 27, 2004[,] Federal Property and Administrative Act of 1949, as amended[,] Executive Order 10450—Security Requirements for Government Employees[,] Executive Order 10865—Safeguarding Classified Information Within Industry[,] Executive Order 12958—Classified National Security Information[,] Executive Order 12968—Access to Classified Information[,] Executive Order 12829—National Industrial Security Program[,] and 5 CFR 731—OPM part 731, Suitability").

323. *See* Homeland Security Act of 2002, 6 U.S.C. § 121(a)–(d) (2006) (creating an Office of Intelligence and Analysis within DHS and giving it the responsibility of accessing, receiving, and analyzing law enforcement information, intelligence information, and other information from local, state, and federal agencies, as well as private sector entities, with an eye towards integrating such information in support of the Department's responsibilities as well as those of the National Counterterrorism Center); *id.* §§ 141, 121(d)(11)–(12) (2006 & Supp. IV 2011) (giving DHS the authority to disseminate information to other federal agencies, as well as state and local government—and private actors—with the only meaningful restriction being that it be done consistent with the protection of intelligence sources and methods as established by the director of National Intelligence, as well as the protection of sensitive law enforcement information consistent with guidelines established by the Attorney General); *id.* § 121(d)(14) (giving DHS the authority to establish and utilize advanced technologies "including data-mining and other advanced analytical tools, in order to access, receive, and analyze data and information in

and Department of Defense[324] each have broad authority to collect personally identifiable information on U.S. citizens. To DHS, in particular, Congress has provided explicit authority to develop new technologies to acquire and store information relevant to any of its law enforcement, border, or national security functions.[325] Specific biometrics provisions supplement these

furtherance of" the Department's responsibilities "and to disseminate information acquired and analyzed by the Department, as appropriate").

324. Outside of war, DoD does not appear to have the general authority to collect personally identifiable information on U.S. citizens within domestic bounds. *Cf.* 10 U.S.C. § 3013 (2006) (authorizing the DoD to collect information only for the Department of the Army). Information-sharing instruments, however, allow it to access information obtained by other federal agencies. *See, e.g.*, Exec. Order No. 13,356, Strengthening the Sharing of Terrorism Information to Protect Americans, 69 Fed. Reg. 53,599 (Sept. 1, 2004). DoD does have primary authority to collect information on active enlisted personnel, such as the Total Army Personnel Database Active Enlisted. *See* DEP'T OF DEF., PRIVACY IMPACT ASSESSMENT (PIA) FOR THE TOTAL ARMY PERSONNEL DATABASE ACTIVE ENLISTED (TAPDB-AE) 3 (2008), *available at* http://ciog6.army.mil/Portals/1/PIA/TAPDB-AE_2010-07-30-101117.pdf (relying on the following legal authority: "10 U.S.C. 3013, Secretary of the Army[,] Army Regulation 600-8-6, Personnel Accounting and Strength Reporting[,] and E.O. 9397 as amended (SSN)"); *see also* PRIVACY IMPACT ASSESSMENT (PIA) FOR THE INSTALLATION ACCESS CONTROL SYSTEM—DRUM 3 (2008), *available at* http://ciog6.army.mil/Portals/1/PIA/IACS-DRUM_23JUN2010.pdf (relying on the following legal authority: "10 U.S.C. 3013, Secretary of the Army[,] Army Regulation 190-13, The Army Physical Security Program and E.O. 9397, as amended (SSN)"). Numerous Executive Orders reach the same purpose. *See, e.g.*, HSPD-12, *supra* note 171; OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, MEMORANDUM NO. M-05-05, ELECTRONIC SIGNATURES: HOW TO MITIGATE THE RISK OF COMMERCIAL MANAGED SERVICES (Dec. 20, 2004), *available at* http://georgewbush-whitehouse.archives.gov/omb/memoranda/fy2005/m05-05.pdf; DEP'T OF DEF., DIRECTIVE NO. 1000.25, DOD PERSONNEL IDENTITY PROTECTION (PIP) PROGRAM (July 19, 2004), *available at* http://www.dtic.mil/whs/directives/corres/pdf/100025p.pdf. DoD also cites a number of Executive Orders in support of its general collection of biometric data. *See* DEP'T OF DEF., MEMORANDUM NO. DTM-05-006, DOD POLICY FOR BIOMETRIC INFORMATION FOR ACCESS TO U.S. INSTALLATIONS AND FACILITIES IN IRAQ (July 15, 2005), *available at* http://www.dtic.mil/whs/directives/corres/pdf/dsd050715iraq.pdf (relying on the legal authority of "HSPD-6 . . . HSPD-11 . . . [, and] Exec. Order 13,356").

325. *See, e.g.*, 6 U.S.C. § 202(1)–(4) (2006) (giving the Secretary of DHS responsibility for securing the borders); 8 U.S.C. § 1103(a)(1) (2006) (granting the Secretary of Homeland Security the administration and enforcement of all laws relating to the immigration and naturalization of aliens and U.S. borders); IDENT System of Records, 72 Fed. Reg. 31,080, 31,081 (June 5, 2007) (giving DHS special authority with regard to the borders, as well as biometric collection and analysis systems); *see also* 8 U.S.C. § 1225(b) (2006) (screening and asylum considerations), *subsection (b)(1)(D) invalidated by* United States v. Barajas-Alvarado, 655 F.3d 1077, 1087 (9th Cir. 2011). As with other departments, myriad other sections of the code underscore the Department's role in this area. *See, e.g.*, 8 U.S.C. § 1324(e) (2006) (discussing outreach program

broader powers.[326] DHS is further empowered to mine such information and then share it with any federal, state, or local entities, or private actors, deemed necessary.[327] Intelligence agencies appear to have similarly broad authority that could be applied to PII.[328] The limits established, however, all but disappear when confronted by the types of programs under question.

for DHS to work with the State Department and the Attorney General to address the issue of U.S. persons bringing in and harboring aliens*); id.* § 1357(h) (2006) (focusing on the protection of juveniles applying to the Secretary of Homeland Security for consent for special immigrant status).

326. New legislation in 2004 required the Secretary of Homeland Security to "develop a plan to accelerate the full implementation of an automated biometric entry and exit data system." Intelligence Reform and Terrorism Act of 2004, Pub. L. No. 108-458, § 4042(a), 118 Stat. 3638, 3724 (to be codified at 8 U.S.C. § 1365b(c)(1)). Congress demanded that the Secretary submit a report detailing the current functionality of the entry and exit data system (including a list of ports of entry and other DHS and Department of State locations where biometric entry data systems were in use, and a listing of the databases and data systems with which the entry and exist data system were interoperable), as well as what resources would be required to resolve any deficiencies in the current system. *Id.* § 7206, 118 Stat. at 3818 (to be codified at 8 U.S.C. § 1365b(c)(2)). The statute required that by December 26, 2007, the new biometric program would be up and running, with a phased implementation of a registered traveler program to take place soon thereafter. *Id.*

The U.S. Coast Guard's collection of personally identifiable information supports its law enforcement and other missions. *See* 14 U.S.C. § 2 (2006) (U.S. Coast Guard Primary Duties); *id.* § 89 (2006) (U.S. Coast Guard Law Enforcement); 19 U.S.C. § 482(a) (2006) (search of vehicles and persons). The agency, in turn, functions within DHS's broader grant of authority for the collection and analysis of biometric and other data. *See* discussion *infra* Part II.A.2. The specific biometric programs discussed above, US-VISIT and IDENT, cite overlapping statutory authorities that enable the collection of PII for the purposes so stated. For example, the PIAs for US-VISIT list the following statutory authority: "the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Public Law 104-208; The Immigration and Naturalization Service Data Management Improvement Act of 2000 (DMIA), Public Law 106-215; The Visa Waiver Permanent Program Act of 2000 (VWPPA), Public Law 106-396; The USA PATRIOT Act, Public Law 107-56; and The Enhanced Border Security and Visa Entry Reform Act ('Border Security Act'), Public Law 107-173," and "[t]he Intelligence Reform and Terrorism Prevention Act of 2004, (IRTPA) Public Law 108-458, § 7208." DHS, UPDATE FOR US-VISIT, *supra* note 115, at 15 n.10; DHS, VISITOR AND IMMIGRANT STATUS, *supra* note 120, at 4 n.3. For IDENT, the statutory authority for maintenance of the system turns on the authorities of each agency that contributes to the IDENT database. *See* Privacy Act; IDENT System of Records, 72 Fed. Reg. 31,080, 31,081 (June 5, 2007) (listing as statutory authority: "6 U.S.C. 202, 8 U.S.C. 1103, 1158, 1201, 1225, 1324, 1357, 1360, 1365a, 1365b, 1379 . . . 1732; [and] 19 U.S.C. 1589a").

327. 6 U.S.C. § 124h (2006).

328. Amendments to the 1947 National Security Act instruct the Director of National Intelligence to determine the requirements and priorities for, and manage and direct the collection, analysis, production, and dissemination of,

1. Privacy Act of 1974 and Systems of Records Notice

The Privacy Act of 1974 is the main legislation governing the federal collection, use, and disclosure of personally identifiable information.[329] The statute falls short, however, of providing for robust protection of the types of technologies that mark the biometrics realm. Reporting requirements, for instance, are limited to data associated with specific individuals.[330] The act only applies to federal entities—not state and local governments.[331] And only U.S. citizens and permanent residents fall within the legislation's requirements.[332]

national intelligence, and intelligence related to national security—understood as:

> [A]ll intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that . . . pertains . . . to more than one United States Government agency; and that involves—(i) threats to the United States, its people, property, or interests; (ii) the development, proliferation, or use of weapons of mass destruction; or (iii) any other matter bearing on United States national or homeland security.

50 U.S.C. § 401a(5) (2006). The intelligence community undertaking the collection, analysis, and dissemination of such information includes the Office of the Director of National Intelligence, CIA, National Security Agency, Defense Intelligence Agency, National Geospatial-Intelligence Agency, National Reconnaissance Office, other DoD offices conducting reconnaissance, the intelligence elements of the Army, Navy, Air Force, and USMC, FBI, the Drug Enforcement Agency (DEA), the Department of Energy, the Bureau of Intelligence and Research at the Department of State, the Office of Intelligence and Analysis of the Department of the Treasury, elements of DHS concerned with the analysis of intelligence information (including the Coast Guard), and any other entities designated by the President. *Id.* § 401a(4). Agencies use information-gathering functions to bypass limits that might otherwise apply to agencies' collection of PII. The CIA, for instance, is statutorily prevented from assuming any police, subpoena, or law enforcement powers or internal security functions. 5 U.S.C. § 403-3(d)(1) (2006). It is not clear, however, precisely what the CIA can and cannot do within its broader authorities. *See* Grant T. Harris, Note, *The CIA Mandate and the War on Terror*, 23 YALE L. & POL'Y REV. 529, 532–33 (2005). Similarly, Executive Order 12,333 of 1981 and Attorney General guidelines restrict the CIA in its collection of information about U.S. citizens: it is only allowed to collect information for an authorized intelligence purpose, amongst which international terrorism is included. *See* Exec. Order No. 12,333, 46 Fed. Reg. 59,941, 59,950 (Dec. 8, 1981). Exactly what constitutes international terrorism, however, is not clear—nor do there appear to be any limits on whether the individual about whom the information is sought be the target of the investigation, or merely related in some way to an investigation itself. *See id.* (failing to define "international terrorism").

329. 5 U.S.C. § 552a (2006).

330. *Id.* § 552a(b).

331. *See id.* § 552a(b) (applying restrictions to an "agency," not a "non-federal agency").

332. *Id.* § 552a(a)(2).

Not all data collection qualifies for protection. Instead, notice must only be provided for information contained in a "system of records."[333] The Act defines a "record" as:

> [A]ny item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph . . . .[334]

A record is thus created where biometric information, such as fingerprint, voice, or facial recognition data, is stored and assigned to a particular individual.[335] A "system of records" is understood then as "a group of any records . . . from which information is retrieved by the name of the individual . . . or other identifying particular."[336] So, where the government maintains a group of biometric records, from which information is retrievable by a marker assigned to an individual in regard to whom the information is stored, it is maintaining a system of records and is thus, at the outset, subject to the Privacy Act's provisions.[337]

On the other hand, if the government maintains a video surveillance program in which it stores the biometric information of passersby, without correlating such information to particular individuals, such a system does not appear to fall within the Privacy Act. The linking of data to individuals is essential to the formation of a "record."[338] Nor does the statute appear to apply to automated video- or photo-matching systems, which would merely correlate images, without tying them to particular persons. A system of records thus occurs only at the point "when agencies use the Privacy Act record as a key to retrieve information from these files."[339] *Pari passu*, the legisla-

333. *See id.* § 552a(d).

334. *Id.* § 552a(a)(4).

335. *Id.*

336. *Id.* § 552a(a)(5).

337. The fact that the agency has the capability to retrieve individual records does not subject it to the provisions of the Privacy Act. Privacy Act Guidelines, 40 Fed. Reg. 28,949, 28,952 (July 9, 1975); Privacy Act of 1974, 52 Fed. Reg. 12,990, 12,991 (Apr. 20, 1987). Rather, the agency must actually retrieve records by an identifying particular. Privacy Act Guidelines, 40 Fed. Reg. at 28,952; Privacy Act of 1974, 52 Fed. Reg. at 12,991.

338. Privacy Act of 1974, 52 Fed. Reg. at 12,991 ("In order to carry out . . . call detail programs, agencies will have to link numbers and names so that they can determine who is responsible for what call. It is at this point, that the telephone number meets the Privacy Act definition of a 'record.'").

339. *Id.*

tion appears *not* to apply to programs focused on developing biometric technology through the widespread accumulation of data that is not tied to particular individuals.

Under the statute, each agency maintaining personally identifiable databases must publish a system of records notice (SORN) in the Federal Register.[340] SORNs may be issued in regard to federal government-wide initiatives, as well as department-wide programs and sub-department agency initiatives.[341] All federal agencies must adopt and publish minimum standards with respect to the collection, maintenance, use and dissemination of personal information contained in such systems.[342] The legislation restricts the transfer of data absent a written request by or with the prior consent of the individual to whom the information pertains unless such a request is made by another government agency head, so long as the agency head makes a written request which maintains the record specifying the specific portion desired, and the purpose for which the record is sought.[343]

Outside of specified (albeit broad) exemptions, discussed below, upon request, the legislation requires each agency that maintains a system of records to grant access to the individual from whom the information was collected, in order to give the target the opportunity to correct any errors in the information.[344] The agency must then either promptly correct the portion of the record considered inaccurate, irrelevant, untimely or incomplete, or promptly inform the individual of its refusal to amend the record and the appeals process to be followed.[345]

340. 5 U.S.C. § 552a(e)(4).

341. SORNs, for instance, have issued not just from the DHS as a whole, but also from DHS's sub-departments: Customs and Border Protection, Federal Emergency Management Agency, Intelligence and Analysis Unit, Immigration and Customs Enforcement, the National Protection and Programs Directorate, the Office of Health Affairs, the Office of Inspector General, Operations, Science and Technology, the Transportation Security Administration, Citizenship and Immigration Services Ombudsman, U.S. Citizenship and Immigration Services, U.S. Coast Guard, and U.S. Secret Service. *See System of Records Notices (SORNs)*, U.S. DEP'T OF HOMELAND SEC., http://www.dhs.gov/system-records-notices-sorns (last visited Nov. 2, 2012) (listing all general federal, departmental, and sub-agency SORNs related to DHS).

342. 5 U.S.C § 552a(e)–(f).

343. *Id.* § 552a(b)(7).

344. *Id.* § 552a(d)(1).

345. *Id.* § 552a(d)(2)(B). The statute sets a limit of ten days either to make the corrections or to notify the individual that the information will remain untouched. *Id.* § 552a(d)(2)(A).

Two important points about this legislation, outside of the exemptions, deserve notice. First, the statute does not regulate state and local governments or private entities. Thus, *any biometric information gathered by state or local governments is exempted from the Act's requirements*.[346] The agency using such data is only subject to the much weaker expectation of due diligence[347] and is under no statutory obligation to inform the individual that personally identifiable information has been collected on the target or to correct any errors in the same.[348] IAFIS, for instance, is part of the Fingerprint Identification Records System, portions of which are exempt from access and amendment under the Privacy Act.[349] This database relies in part on local law enforcement fingerprint data, which does not fall subject to the Privacy Act. Thus, while the FBI's role in maintaining and disseminating the identification records carries the responsibility of undertaking such activities in a responsible manner,[350] any errors in the state collection of biometric data are not subject to the same amendment requirements as federally-generated information.[351]

Second, the Privacy Act applies only to U.S. citizens and not to companies, non-resident aliens, or foreigners.[352] The purpose of this limitation was, in part, to ensure the exclusion of economic regulatory activity, as well as intelligence files and databases devoted to foreign nationals, "or maintained by the

346. *Id.* Federal agencies implementing biometric programs cite this exception—the PIA, for instance, issued by the FBI in regard to the Repository for Individuals of Special Concern, specifically notes that "[t]he user agencies that contribute the underlying information to the NGI and NCIC [National Crime Information Center] likely do not provide any sort of Privacy Act Statements or similar actual notice to the individuals from whom or about whom the information pertains. This is because non-federal contributors are not subject to the Privacy Act, federal contributors are usually exempted from the Privacy Act's individual collection notice provisions in connection with criminal law enforcement activities, and/or provision of individual notice incident to criminal law enforcement activities is typically impracticable." RISC PIA, *supra* note 201, § 6.1.

347. *See* 5 U.S.C. § 552(a)(6)(C)(i).

348. *See supra* note 344 and accompanying text.

349. 28 C.F.R. § 16.96(e), (f) (2010).

350. *See* Tarlton v. Saxbe, 507 F.2d 1116, 1122 (D.C. Cir. 1974); Menard v. Saxbe, 498 F.2d 1017, 1028–29 (D.C. Cir. 1974).

351. *Cf.* Shadd v. United States, 389 F. Supp. 721, 724 (W.D. Pa. 1975) (suggesting that the FBI may have less of a duty to correct errors resulting from state collection of information), *aff'd mem.* 535 F.2d 1247 (3d Cir. 1976).

352. Congress accomplished this limitation through the definition of "individual" as "a citizen of the United States or an alien lawfully admitted for permanent residence." *See* 5 U.S.C. § 552a(a)(2) (2006).

State Department, the Central Intelligence Agency and other agencies for the purpose of dealing with nonresident aliens and people in other countries."[353] Thus, biometrics systems relating to non-citizens entering and leaving the country, living within U.S. bounds, or located overseas, fall entirely outside the statute.

2. Exemptions to the Privacy Act

The Privacy Act contains a number of general and specific exceptions, which prove particularly important in the realm of RBI. It could be argued that they obliterate any substantive impact that the Privacy Act might otherwise have on this rapidly-emerging field.

First, the statute provides a general exemption for records maintained by the CIA.[354] Although this provision is permissive—not required—it provides for the head of any agency to promulgate rules to exempt (with some exceptions) systems of records maintained by the intelligence agency.[355] Thus, biometric programs launched by the CIA—targeting U.S. citizens or non-citizens—could develop outside important aspects of the Privacy Act's protections.

The CIA, for instance, is not required to provide individuals with access to records.[356] It is not required to establish and promulgate procedures whereby an individual can be notified (at the individual's request) if the system of records contains a

353. S. REP. NO. 93-1183, at 75 (1974), *reprinted in* 1974 U.S.C.C.A.N. 6916, 6993.

354. 5 U.S.C. § 552a(j)(1).

355. *Id.* The exceptions include: subsection (b) (relating to the conditions of disclosure); subsections (c)(1) & (2) (requiring agencies to keep an accurate accounting of the date, nature or purpose of any disclosures of the records and the name/address of the person/agency to whom the disclosure is made); and subsection (e)(4)(A)–(F) (publication in the Federal Register of the existence and nature of the system). *Id.*; *see also* H.R. REP. NO. 93-1416, at 19 (1974), *reprinted in* 1974 U.S.C.C.A.N. 6916, 6931 ("The Committee also wishes to stress that this section is not intended to require the C.I.A. and criminal justice agencies to withhold all their personal records from the individuals to whom they pertain. We urge those agencies to keep open whatever files are presently open and to make available in the future whatever files can be made available without clearly infringing on the ability of the agencies to fulfill their missions.").

356. The following sections are included in the CIA's general exemption from the requirements of the Privacy Act: 5 U.S.C. § 552a(c)(3)–(4) (requiring an agency to disclose the information made in a request) and 5 U.S.C. § 552a(d) (requiring each agency maintain records but exempted by the CIA). *See id.* § 552a(j).

record pertaining to him; nor must the agency provide procedures on how to gain access to the records or to contest their content.[357] The CIA is not required to reveal the categories of records in the system.[358] Nor must it maintain records "with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness."[359] The agency cannot be subject to civil remedies for failing to comply with requests to obtain information or to amend records; nor may a court order the agency to amend the individual's record in any way.[360] The courts similarly may not enjoin the CIA from withholding records and order the production to the complainant.[361]

A second general exemption exists for criminal law enforcement records.[362] The legislation allows law enforcement agencies to exempt records relating to the identification of criminal offenders and alleged offenders, data compiled for criminal investigations, and reports developed at any stage of the criminal law process from arrest or indictment through release from supervision.[363]

Specific exemptions, located under subsection (k) of the legislation, further reflect the statute's general aversion to regulating matters related to national security. The head of any federal agency may promulgate rules to exempt certain record systems where they deal with classified information or the

357. The following sections are similarly included in the general exemptions for the CIA pursuant to 5 U.S.C. § 552a(j)(1) of the Privacy Act: § 552a(e)(4)(G)–(H) (requiring the agency to notify an individual that a record is being kept on him or her upon requires) and § 552a(f) (requiring the agency to establish rules to carry out the provisions of the section). *See also id.* § 552a(e)(8) (reasonable effort to serve notice not required to be provided to individuals included in the system of records when any record is made available to any person under compulsory legal process when such process becomes a matter of public record).

358. The CIA's exemption also includes § 552a(e)(4)(I) (requiring an agency to maintain only information about an individual that is relevant to that agency's purpose). *Id.* § 552a(j)(1).

359. *Id.* § 552a(e)(5).

360. The CIA's exemption also includes § 552a(g)(1)–(2) which makes an agency liable under civil remedies for failing to comply with information requests or to amend records. *Id.* § 552a(j)(1).

361. Section 552a(g)(3), allowing a court to enjoin an agency from withholding records, is also included the CIA exemption pursuant to 5 U.S.C. § 552a(j)(1). *Id.* Note, however, that criminal penalties for misuse of the information may still apply. *See id.*

362. *Id.* § 552a(j)(2).

363. *Id.*

identity of informers.[364] Under such circumstances, the federal agency may prevent information about the records from being made available to the individual named in the record.[365] It is not, moreover, required to maintain only such information "as is relevant and necessary to accomplish a purpose of the agency" as required by statute or Executive Order.[366] Precisely on such grounds, biometric systems have already been exempted from the Privacy Act via notices published in the Federal Register.[367] The statute also allows for a specific exemption for "other administrative purposes"—a provision that has already been put to use.[368]

The Department of Homeland Security's automated biometric identification system, for instance, incorporates information pertaining to civil and criminal law, including immigration, investigations, national security, and intelligence activities.[369] It also contains unique identifiers and encounter history information which is used to place the biometric information in context.[370] The information is collected by or on behalf of DHS and its components and may contain personally identifiable data collected by domestic or foreign intelligence agencies.[371] In July 2006, DHS published a notice of proposed rulemaking to exempt portions of IDENT from one or more provisions in the Privacy Act.[372] No responses were received by the Department, which made the rule final within a year of its initial filing.[373]

DHS made use of its overlapping authorities to claim multiple exemptions. The waiver, it claimed, was necessary to protect national security, immigration, border management, and

364. *Id.* § 552a(k)(5).

365. *See id.* (exempting 5 U.S.C. § 552a(c)(3), § 552a(d), and § 552a(e)(4)(G)–(I)). Note also that the agency is therefore not required to establish procedures and rules whereby individuals can be notified as to whether such records are being maintained in regard to the individual or the procedures to be followed to gain access to the same. *See id.* (exempting 5 U.S.C. § 552a(f)).

366. *Id.* (exempting 5 U.S.C. § 552a(e)(1)).

367. *See infra* notes 371–78, 403–14 and accompanying text.

368. 5 U.S.C. § 552a(b)(1)–(12).

369. Privacy Act of 1974: Implementation of Exemptions, 72 Fed. Reg. 38,749 (July 16, 2007) (to be codified at 6 C.F.R. pt. 5).

370. *Id.*

371. *Id.* at 38,751.

372. *Id.*

373. *Id.*

law enforcement activities.[374] The Department evinced further concern that revealing such data would undermine the physical safety of informants and officials and lead to the release of classified information.[375] Additionally, DHS stated, "[d]isclosure of information to the subject of the inquiry could also permit the subject to avoid detection or apprehension."[376] DHS followed this notice with a second proposal for rulemaking in July 2011, exempting the terrorist screening database from Privacy Act requirements because of criminal, civil, and administrative enforcement requirements.[377] It applies, inter alia, to the US-VISIT program for inclusion into the DHS Enterprise Biometrics Service.[378] Various other exemptions have been invoked for programs collecting biometric and other data.[379]

Later amendments to the Privacy Act have done little to increase its traction with regard to biometric collection systems. In 1988, for instance, Congress amended the Privacy Act to address the use of records in automated matching programs.[380] This statute added procedural requirements for agencies to follow regarding computer matching activities.[381] It provided for notice and the opportunity to refute adverse information before denial or termination of a benefit.[382] The legislation also required that agencies create data protection boards to oversee their computer matching activities.[383] Each agency proposing to make significant changes in their records systems or matching programs became required to provide adequate notice to the Committee on Government Operations of

374. *Id.*

375. *Id.*

376. Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/ALL—030 Use of the Terrorist Screening Database System of Records, 76 Fed. Reg. 39,315, 39,316 (July 6, 2011) (to be codified at 6 C.F.R. pt. 5).

377. *Id.* at 39,315.

378. *Id.* at 39,316.

379. *See, e.g.*, 75 Fed. Reg. 5,487 (Feb. 3, 2010) (to be codified at 6 C.F.R. pt. 5) (exempting most of the data incorporated into the Automated Targeting System-Passenger from Privacy Act requirements related to access to information, opportunities to challenge data, and collection of information).

380. Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503, § 5, 102 Stat. 2507, 2512–13 (codified as amended at 5 U.S.C. § 552a(o)).

381. 5 U.S.C. § 552a(o)(1) (2006).

382. *Id.* § 552a(o)(1)(D).

383. U.S. DEP'T OF JUSTICE, OVERVIEW OF THE PRIVACY ACT OF 1974, at 3 (2010), *available at* http://www.justice.gov/opcl/1974privacyact.pdf; *see* 5 U.S.C. § 552a(a)(8)–(13), (e)(12), (o), (p), (q), (r), (u) (2006).

the U.S. House of Representatives, the Committee on Governmental Affairs of the Senate, and the Office of Management and Budget, in order to facilitate an examination of the impact on individual privacy rights.[384] Two years later, Congress enacted the Computer Matching and Privacy Protection Amendments of 1990.[385] The statute clarified due process protections; however, the exemptions still apply.

3. E-Government Act of 2002

The E-Government Act of 2002[386] ostensibly further enhanced protection of personal information. Signed by President George W. Bush in December 2002, the legislation entered into force in April 2003.[387] The statute requires that agencies engaged in collecting personal information issue a PIA prior to developing or procuring technologies that collect, maintain, or disseminate personally identifiable information from or about members of the public.[388] While the changes did not address continual monitoring of programs underway, their design was to provide notice *that* such programs were being *initiated*. Any major systems changes entailing new privacy risks would require the publication of new PIAs.[389] Examples might include converting paper-based fingerprint systems to electronic databases or the use of new technologies to significantly alter how information is managed in the system—such as by using new relational database technologies or web-based processing to access multiple data stores for biometric and other data.[390] Similarly, significant merging of government databases would require a PIA, as would new interagency activities.[391] Other examples might include an alteration in the character of data or when new biometric or video surveillance information—or, indeed, contextual data—is added to the system.[392]

384. 5 U.S.C. § 552a(r) (2006).

385. Computer Matching and Privacy Protection Amendments of 1990, Pub. L. No. 101-508, § 7201, 104 Stat. 1388-334, 1388-334–35 (codified as amended at 5 U.S.C. 522a(p)).

386. E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899.

387. *Id.*

388. *Id.* § 208, 116 Stat. at 2921–23.

389. *See, e.g.*, Memorandum from Joshua B. Bolten, Dir., OMB, to Heads of Exec. Dep'ts & Agencies, attachments A, B (Sept. 26, 2003) [hereinafter Bolten Memo], *available at* http://www.whitehouse.gov/omb/memoranda_m03-22/#4.

390. *See id.*

391. *Id.*

392. *Id.*

PIAs must analyze and describe the information to be collected (e.g., its nature and source), why the information is being collected, what its intended use is, with whom the information will be shared, what opportunities individuals have to deny or grant consent, how the information will be secured, and whether the initiative satisfies the definition of a system of records under the Privacy Act.[393] PIAs must then consider the impact of the system on individual privacy.[394]

The statute, however, once again reflected congressional aversion to providing public oversight of matters related to national security. The statute allows for public dissemination of the PIA to be suspended for security reasons or to protect classified (i.e., national security), sensitive (e.g., potentially damaging to a national interest, law enforcement, or free competition), or private information.[395] Under the legislation, national security systems are understood as telecommunications or information systems:

> [O]perated by the Federal Government, the function, operation, or use of which—(A) involves intelligence activities; (B) involves cryptologic activities related to national security; (C) involves command and control of military forces; (D) involves equipment that is an integral part of a weapon or weapons system; or (E) subject to paragraph (2), is critical to the direct fulfillment of military or intelligence missions.[396]

The head of the agency or a designee may limit notice and reporting of tracking activities initiated by the agency which relate to authorized law enforcement, national security, and/or homeland security purposes.[397]

4. Oversight and Guidance

In light of the exemptions embedded in the legislation, one possible recourse for ensuring that agencies do not overreach might be through oversight bodies. Here, the White House Office of Management and Budget (OMB) bears the responsibility for overseeing implementation of the Privacy Act and the PIAs.[398] The role of this agency, however, has been extremely

393. *Id.*

394. *Id.*

395. E-Government Act of 2002, Pub. L. No. 107-347, § 208(a)–(b), 116 Stat. 2899, 2921–22; *see also* Bolten Memo *supra* note 389, at attachments A, C.

396. 40 U.S.C. § 11103(a)(1) (2006).

397. Bolten Memo, *supra* note 389.

398. *See* Guidance on Privacy Act Implications of "Call Detail" Programs, 52 Fed. Reg. 12,290, 12,290 (Apr. 15, 1987); Guidelines on the Relationship of the Debt Collection Act of 1982 to the Privacy Act of 1974, 48 Fed. Reg. 15,556,

deferential to agencies exercising their powers of exemption. No recourse, moreover, to the courts exists. Executive agencies, in turn, have attempted to expand their authorities further by using exemptions in the Privacy Act to block requests for data under the Freedom of Information Act (FOIA).

Under guidelines issued in 1975, OMB explained that the purpose of the measure was "to assure that personal information about individuals collected by Federal agencies is limited to that which is legally authorized and necessary and is maintained in a manner which precludes unwarranted intrusions upon individual privacy."[399] The agency nevertheless gave enormous deference to the exemptions included in the act, mentioning them dozens of times with little or no further comment.[400] OMB also further expanded its reach, noting that the exemption which provided for notice of disclosure for "routine uses" could extend to foreign as well as state and local entities.[401] Records exempted from the Act's requirements could still "be disseminated to other agencies and incorporated into their non-exempt records systems" where they would continue to be exempt from notice and challenge.[402]

15,556 (Apr. 11, 1983); Office of Mgmt. & Budget: Implementation of the Privacy Act of 1974, 40 Fed. Reg. 56,741, 56,741 (Dec. 4, 1975); Heads of Executive Departments and Establishments: Responsibilities for the Maintenance of Records About Individuals by Federal Agencies, 40 Fed. Reg. 28,948, 28,948 (July 9, 1975); Memorandum from Robert P. Bedell, Deputy Adm'r, Office of Info. & Regulatory Affairs, to the Senior Agency Officials for Info. Res. Mgmt., 7 (May 24, 1985) [hereinafter Bedell Memo] (providing an update of Privacy Act Guidance); Bolten Memo, *supra* note 389; Memorandum from Jacob J. Lew, Dir. of the OMB, to Heads of Exec. Dep'ts & Agencies (Dec. 20, 2000), *available at* http://georgewbush-whitehouse.archives.gov/omb/memoranda/m01-05.html; Memorandum from Sally Katzen, OMB, to Chief Information Officers (Nov. 3, 1997) *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/katzen_prwora.pdf; Memorandum from James T. Lynn, Dir. OMB, to Heads of Exec. Dep'ts & Agencies (Oct. 3, 1975).

399. Responsibilities for the Maintenance of Records About Individuals by Federal Agencies, 40 Fed. Reg. 28,948, 28,948 (July 9, 1975).

400. *See, e.g.*, *id.* at 28,950 (listing the exemptions); *id.* at 28,954 (noting that an agency may not rely on a provision in FOIA for "refusing access to a record to the individual to whom it pertains, unless such refusal of access is authorized by an exemption within the Privacy Act"); *id.* at 28,956 (requiring that information be provided upon inquiry "unless the system has been exempted from this provision pursuant to subsections (j) or (k)"); *id.* at 28,957 (discussing denial of access and carving out an exception for the exemptions). For examples where OMB directly discussed the sections covering the exemptions see *id.* at 28,971–73 (noting the exemption of CIA and criminal law enforcement records).

401. *Id.* at 28,955.

402. *Id.* at 28,971.

OMB noted that while judicial review could be sought for specific exemptions, no recourse to the courts could be sought for the general exemptions within the Act.[403] Even the provision of judicial review of exemptions under subsection (k) was subject to conditions that diminished its effectiveness. For one, it was undermined by the initial decision to exempt the system of records: it would be difficult to even know about, much less to establish standing with regard to, a secret system of records. While notice might be required of the existence of the exemption, such notice could be abbreviated and made rather cryptic in its form.[404] OMB explained that the only information that had to be released was the name of the system, the specific provisions of the Act from which the system was to be exempted, and a general explanation of why.[405] For another, even where the existence of and details about such systems could be established, the courts were to narrowly consider "the propriety of the exemption which denies him access to his files."[406] That is, the courts could only inquire into whether the exemption itself could be justified—not the particular case at hand.[407] In the realm of national security, assumedly, there would be little reason to question whether such an exemption was a legitimate exercise of state authority.[408]

Starting in 1980, the Department of Justice began using the exemptions in numerous statutes governing disclosure to block requests submitted under the Freedom of Information Act.[409] In March 1984, OMB conformed its "guidance" on the re-

403. *Id.* at 28,969 (noting "that systems of records covered under subsection (j) (general exemptions) are permitted to be exempted from" judicial review).

404. *See* Responsibilities for the Maintenance of Records About Individuals by Federal Agencies, 40 Fed. Reg. at 28,948, 28,970 (July 9, 1975) (discussing subsections (a)(5), definitions, and (e)(4), public notice); *see also id.* at 28,971 (noting that a description of the system to be exempted should only be described where "possible").

405. *Id.* at 28,971.

406. *Id.* at 28,969 (quoting S. REP. NO. 93-1183, at 82 (1974)).

407. OMB explained that, consistent with the Senate Report,"[i]n deciding whether the citizen has a right to see his file or to learn whether the agency has a file on him, the court would of necessity have to decide the legitimacy of the agency's reasons for the denial of access, or refusal of an answer." S. REP. NO. 93-1183, at 82 (1974), *reprinted in* 1974 U.S.C.C.A.N. 6916, 6996.

408. In 1975, OMB issued further guidance, noting that the procedures for denials of requests to amend a record did not need to include a justice or judge; instead, any agency official meeting the statutory criteria would suffice. Implementation of the Privacy Act of 1974, 40 Fed. Reg. 56,741, 56,743 (Dec. 4, 1975). Statutory criteria are laid out in 5 U.S.C. § 2104(a) (2006).

409. *See, e.g.*, Doug Letter et al., *Business Confidentiality After Chrysler*,

lationship between the Privacy Act and FOIA to the Government's litigating position, publishing the change in the Federal Register.[410] The circuits subsequently split: the Third Circuit and the D.C. Circuit rejected the Government's argument, while the Fifth and Seventh largely agreed that the Privacy Act should be considered a FOIA (b)(3) statute.[411] In 1984, the Supreme Court was set to hear argument on the question, but before it could do so, Congress passed legislation amending the Privacy Act to exclude the statute from FOIA (b)(3) considerations.[412] OMB subsequently amended its guidance to conform to the new statute, erecting a wall between the two pieces of legislation.[413] Where requests cited the Privacy Act, they would be processed under that legislation alone; where they cited FOIA, they would be processed under that statute alone; and where they cited both or neither, two analyses would have to follow in considering whether to grant the request for information.[414]

As the digital revolution took hold, the executive branch came up with new and innovative ways to avoid the Privacy Act. This forced OMB to issue further guidance on the implications of call detail programs, inter-agency sharing of personal data, and the E-Government Act. OMB recognized the particular challenges posed by new technology, noting in 1987 the same problems that biometrics now pose to the applicability of the statute:

> Rapid growth in automated data processing and telecommunications technologies has created new and special problems relating to the Federal Government's creation and maintenance of information about individuals. At times, the capabilities of these technologies have appeared to run ahead of statutes designed to manage this kind of information, particularly the Privacy Act.[415]

FOIA UPDATE (1980), *available at* http://www.justice.gov/oip/foia_updates/Vol_I_2/page4.htm.

410. Revised Supplemental Guidance on Implementation of the Privacy Act of 1974, 49 Fed. Reg. 12,338, 12,338 (Mar. 29, 1984).

411. *Compare* Provenzano v. U.S. Dep't of Justice, 717 F.2d 799, 800 (3d Cir. 1983), *vacated*, 105 S. Ct. 413 (1984), *with* Shapiro v. Drug Enforcement Agency, 721 F.2d 215, 223 (7th Cir. 1983), *vacated*, 105 S. Ct. 413 (1984), *and* Painter v. FBI, 615 F.2d 689, 690–91 (5th Cir. 1980), *superseded by statute*, CIA Information Act of 1984, Pub. L. No. 98-477, 98 Stat. 2209 (1984) (codified at 5 U.S.C. § 552a), *as recognized in* Ely v. Federal Bureau of Investigation, 781 F.2d 1487 (11th Cir. 1986).

412. *See* H.R. Res. 5164, 98th Cong. (1984) (enacted).

413. *See* Bedell Memo, *supra* note 398.

414. *Id.* at 9.

415. Guidance on Privacy Act Implications of "Call Detail" Programs to Manage Employees' Use of the Government's Telecommunications Systems,

OMB has yet to issue specific guidance on the remote biometric identification systems that are beginning to proliferate.

5. Privacy Impact Assessments Issued in Relation to Biometric Collection Systems

Some PIAs have been issued for government biometric programs. Their chief value appears to be in informing the public that new initiatives aimed at gathering personal information are underway. They do little to address contrary concerns and lack any stringent mechanism to revise the programs. In addition, they are often so broad as to make the issuance of a PIA almost meaningless, in that they allow for significant further growth of the programs absent any further public notification.

Agencies issuing PIAs are under no compulsion to address public concerns raised in the course of the PIA process. Already this effect can be seen in the biometrics realm. Starting in 2004, for instance, the Department of Homeland Security began issuing PIAs for development of its US-VISIT program.[416] US-VISIT soon expanded to become the DHS repository for USCIS biometric (fingerprints and photographs) and biographic data, with its targets extending to include lawful permanent residents, individuals seeking asylum, and other aliens.[417] In response to a notice of proposed rulemaking that paralleled the July 2006 PIA, DHS received a dozen submissions raising privacy concerns particularly in relation to "mission creep" (i.e., concern that US-VISIT was expanding beyond its original purpose in a way that those participating in the program had not anticipated); the lack of judicial review for those impacted by US-VISIT; privacy during the inspection process; and false hits.[418] Responding to claims of mission creep, which appeared to be the area of greatest concern, Paul Hasson, the Acting Pri-

52 Fed. Reg. 12,290, 12,291 (Apr. 20, 1987).

416. *See, e.g.*, U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE UNITED STATES VISITOR AND IMMIGRANT STATUS INDICATOR TECHNOLOGY (US-VISIT) PROGRAM IN CONJUNCTION WITH THE NOTICE OF PROPOSED RULEMAKING ON THE AUTHORITY TO PROCESS ADDITIONAL ALIENS IN US-VISIT 3 (2006) [hereinafter US-VISIT PROPOSED RULEMAKING ON THE AUTHORITY TO PROCESS ADDITIONAL ALIENS], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_addaliens.pdf; DHS, UPDATE FOR US-VISIT, *supra* note 115; DHS, INCREMENT 1, *supra* note 135.

417. *See* US-VISIT PROPOSED RULEMAKING ON THE AUTHORITY TO PROCESS ADDITIONAL ALIENS, *supra* note 416. Note that the program exempts children under the age of fourteen and persons over the age of seventy-nine, but includes lawful U.S. permanent residents. *Id.* at 3.

418. *Id.*

vacy Officer, simply noted that DHS has always anticipated expanding the program to cover all aliens entering the United States.[419]

As if to underscore biometric program expansion, in 2006, US-VISIT partnered with the United States Coast Guard (USCG) to develop new technologies to provide for biometrics collection and analysis capability at sea. Its first PIA, issued in November 2006, announced the Mona Passage Proof of Concept, to be conducted November 2006 through April 2007.[420] The program held national security and law enforcement applications. The aims were to develop biometric capabilities for DHS, to provide information necessary to determine what to do in the case of undocumented alien interdictions, to deter human smuggling, and to help preserve life at sea.[421] Handheld devices obtained fingerprint and digital images, connecting biometric information with biographic data (name, gender, date of birth, nationality, departure point, date of departure, destination point, and identity of the master of the U.S. vessel in question).[422] USCG vessels were equipped with stand-alone computers to correlate IDENT biometric data and associated fingerprint identification numbers with information corresponding to KSTs, aggravated felons, previous deportees, and recidivists from Caribbean countries.[423] DHS updated the PIA in 2007 to reflect the new ability to update the biometric databases located on the vessels by satellite technologies for analysis against the IDENT database.[424] In 2008, DHS issued a new PIA to reflect the expansion of the program at sea, "along with other remote areas where DHS operates."[425] In addition to interdiction

419. *Id.*

420. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE U.S. COAST GUARD "BIOMETRICS AT SEA" MONA PASSAGE PROOF OF CONCEPT 2 (2006), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscg_monapass.pdf. More than forty percent of the undocumented aliens interdicted by the U.S. Coast Guard since 2004 tried to enter the United States illegally through the Mona Passage, located between the Dominican Republic and Puerto Rico. *Id.* at 3.

421. *Id.* at 2.

422. *Id.* at 3–4.

423. *Id.* at 4. The databases would be updated on a regular basis. *Id.*

424. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT UPDATE FOR THE U.S. COAST GUARD "BIOMETRICS AT SEA" PROGRAM 2 (2007), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscg_monapass_update.pdf.

425. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE U.S. COAST GUARD "BIOMETRICS AT SEA" 2 (2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscg_biometrics.pdf.

of undocumented aliens and human trafficking, the systems would be directed toward smuggling, drug interdiction, and other illegal activities, thus including the relevant criminal history as well as other contextual and biographic data.[426] Further updates were issued in 2011, reflecting technological advances in data transfer, storage, and encryption systems.[427]

The U.S. Coast Guard is not the only entity at DHS to issue a PIA for emerging biometric programs. In July 2011, for instance, the Transportation Security Laboratory, which focuses on new technologies to detect and mitigate the threat of improvised explosive devices, issued a PIA that outlined its intended use of iris and fingerprint recognition technology to determine access to the facility.[428]

DOJ, like DHS, has also issued a limited number of PIAs in regard to biometric programs. The first such document appears to have been released in 2004, noting the proposed development of a Biometrics-Reviewer Website/Database.[429] The goal of the program was to develop a prototype using information voluntarily submitted by individuals familiar with biometrics and interested in volunteering to serve on agency review panels.[430] Data to be obtained included name, employment type, employer, biometric experience (e.g., years, type (operational, research and development, test, and evaluation)), and modality

426. *Id.* at 2–3.

427. U.S. DEP'T OF HOMELAND SEC., DHS/USCG/PIA-002(C), PRIVACY IMPACT ASSESSMENT UPDATE FOR THE U.S. COAST GUARD "BIOMETRICS AT SEA" 2 (2011), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscg_bass_update002c.pdf (describing the program's replacement of encrypted flash drives with the use of USB cables and encrypted hard drives to minimize the gap in transferring biometric and biographic data from the system laptop to the onboard computer connected to the USCG Data Network Plus). Note that LEIDB/Pathfinder, another USCG database, does not contain any photographs or biometric data. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE LAW ENFORCEMENT INFO. DATA BASE (LEIDB)/PATHFINDER 6 (2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_leidbpathfinder.pdf.

428. U.S. DEP'T OF HOMELAND SEC., DHS/S&T/PIA-023, PRIVACY IMPACT ASSESSMENT FOR THE BIOMETRICS ACCESS CONTROL SYSTEM AT THE TRANSPORTATION SECURITY LAB 2 (2011), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-st-tsl-bacs.pdf.

429. *Privacy Impact Assessment (PIA): Biometrics-Reviewer Website/Database*, FED. BUREAU OF INVESTIGATION (Dec. 21, 2004), http://www.fbi.gov/foia/privacy-impact-assessments/biometrics [hereinafter FBI, *Biometrics-Reviewer*].

430. *Id.*

(facial recognition, fingerprints, etc.).[431] The information, housed at a contractor facility, would be available to the National Science & Technology Council's Interagency Working Group on Biometrics.[432]

As aforementioned, a strong argument could be made that PIAs provide little by way of limits on the federal development of biometric programs. PIAs for the FBI's Next Generation Identification program, for instance, are incomplete.[433] Thus far, it appears that only two PIAs have been issued specifically in relation to the program, which is designed with seven con-

431. *Id.* "Modality" refers to the application of biometric technologies to different physical attributes. NAT'L SCI. & TECH. COUNCIL COMM. ON TECH. ET AL., PRIVACY AND BIOMETRICS: BUILDING A CONCEPTUAL FOUNDATION 12 (2006), *available at* http://www.biometrics.gov/docs/privacy.pdf. Fingerprint, face, iris, voice, signature, and hand geometry are some examples of the different types of modalities being developed. *Id.*

432. FBI, *Biometrics-Reviewer*, *supra* note 429.

433. Prior PIAs related to the FBI's biometric technologies include: *Privacy Impact Assessment: National Dental Image Repository*, FED. BUREAU OF INVESTIGATION (2006), http://www.fbi.gov/foia/privacy-impact-assessments/ndir (discussing the 2005 creation of the National Dental Image/Information Repository to facilitate the identification of missing, unidentified, and wanted persons by drawing on dental records, photographs, and x-rays of the head and neck region); FBI, *Biometrics-Reviewer*, *supra* note 429; *Privacy Impact Assessment: National DNA Index System (DNS)*, FED. BUREAU OF INVESTIGATION (Feb. 24, 2004), http://www.fbi.gov/foia/privacy-impact-assessments/dns (discussing CODIS and noting that, although a notice for the National DNA Index System had been published in the Federal Register in 1996, a PIA had not previously been submitted); *Privacy Impact Assessment: Computer Aided Facial Recognition Project*, FED. BUREAU OF INVESTIGATION (Feb. 19, 2004), http://www.fbi.gov/foia/privacy-impact-assessments/facial-recognition (detailing a study at the University of Sheffield in England and elsewhere on the statistics of facial landmark geometry); *Privacy Impact Assessment: Integrated Automated Fingerprint Identification System National Security Enhancements*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/foia/privacy-impact-assessments/iafis (last visited Nov. 2, 2012). An additional PIA listed on the FBI website lacks a date, but relates directly to biometric data. *See Privacy Impact Assessment: DOJ/FBI-DHS Interim Data Sharing Model (iDSM)*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/foia/privacy-impact-assessments/idsm (last visited Nov. 2, 2012) (discussing pilot information-sharing initiative between DHS and DOJ/FBI); *see also Privacy Impact Assessment for the Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purposes–Channeling*, FED. BUREAU OF INVESTIGATION, (May 5, 2008), http://www.fbi.gov/foia/privacy-impact-assessments/firs-iafis (discussing the use of biometric data for noncriminal justice purposes); *Privacy Impact Assessment for the eGuardian Threat Tracking System*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/foia/privacy-impact-assessments/eguardian-threat (last visited Nov. 2, 2012) (discussing the use of suspicious activity reports to determine which cases require investigative follow-up).

stituent parts and the incorporation of multiple new technologies in mind.

The first PIA, released in June 2008, focused on the Interstate Photo System (NGI-IPS).[434] The assessment highlighted enhancements to the existing system, such as the ability to retain more photographic images, new opportunities for local, state, and federal agencies to submit photographs, and additional search capabilities, including automated searches using facial recognition technology.[435] Although other government agencies claimed that additional public information they collected would only be used to run against their existing databases, and not kept for further data mining,[436] the FBI's PIA is written to include the retention and future use of such images—even in cases where direct identification from the images is not immediately possible.[437]

The PIA offers little to mitigate concern about the new system beyond the FBI's existing standards and policies.[438] At the same time, it recognizes significant gaps in protection of individual privacy. Individuals may be unaware that their images have been recorded—much less stored.[439] For information submitted by criminal agencies, individuals have no opportunity or right to refuse collection; for civil submissions, refusal to provide information may have an adverse impact on the government benefit being requested.[440] The PIA specifically notes that the FBI is not responsible for authenticating or correcting data in the system.[441] The Bureau's clear aim, moreover, in adopting the system, is to allow the FBI to "provide additional function-

434. *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS)*, *supra* note 18.

435. *Id.* § 1.7.

436. *See supra* text accompanying notes 110–14.

437. *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS)*, *supra* note 18.

438. The PIA recognizes, for instance, that the FBI's existing technology protections, vetting of system users, existing access policies, training requirements, and audit policies will be applied to the new system. *Id.* § 8.1–8.7. In turn, technologies to be incorporated into the IPS in the future will be "carefully assessed and tested prior to implementation to ensure that is [sic] sufficiently reliable to provide the desired benefits and minimize erroneous identifications, coupled with only employing facial recognition technology as an investigative aid and not as a means of positive identification." *Id.* § 9.3.

439. *Id.* § 6.1.

440. *Id.* § 6.2.

441. *See id.* § 7.4 (noting that, because the data on Identification Records is submitted by local, state and federal agencies, those agencies are responsible for authenticating and correcting that data).

ality to further law enforcement needs and keep pace with emerging technologies."[442] It is therefore remarkable that the PIA itself fails to consider the many individual technologies currently involved in IPS in any detail—even as it merely recognizes that future technologies must simply be considered in terms of their level of accuracy, and not on their qualitative impact on knowledge generation.

The second PIA, approved in January 2012, detailed the FBI's deployment of the Repository for Individuals of Special Concern, one of the elements in AFIT (the revised IAFIS).[443] This document similarly underscores the ineffectiveness of the Privacy Act. For instance, the PIA provides no detail on how biometric data obtained from local, state, federal, and foreign entities will be analyzed to determine if it meets the various subcategories for inclusion in the RISC.[444] It reports that information is to be shared with a wide range of DOJ components, as well as external domestic and foreign agencies.[445] The PIA notes that individuals will not generally have the opportunity or the right to decline to provide information—nor will their consent be required.[446] The PIA itself serves as notice to individuals that their information may be contained in the data-

442. *Id.* § 9.3.

443. RISC PIA, *supra* note 201. During a meeting with the author, the FBI suggested that the PIA had been issued in July 2010. As of April 2012, however, no such document was publicly available. Following inquiries and formal requests for the PIA by the Georgetown Law Edward Bennett Library, in July 2012, the FBI placed a PIA on its website, indicating that the document had been approved in January 2012. *See id.*; *see also* NEXT GENERATION IDENTIFICATION, *supra* note 184, at 14 (indicating that the RISC PIA was under consideration by the FBI's Office of the General Counsel as of April 2009).

444. *See* RISC PIA, *supra* note 201, § 1.1 ("The RISC entails a specially collated subset of existing records . . . of known or appropriately suspected terrorists, wanted persons, registered sexual offenders, and other special interest categories warranting more rapid biometric-based responses to inquiring users in time-critical situations . . . .").

445. Within DOJ the primary recipients will be the FBI, the DEA, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the Federal Bureau of Prisons, the U. S. National Central Bureau (INTERPOL), and the United States Marshals Service (USMS). *Id.* § 4.1. It will be shared externally with various authorized federal, state, local, tribal, foreign, or international governmental agencies. *Id.* § 5.1.

446. *Id.* § 6.2 ("Because the information in the RISC subset is collected in connection with law enforcement investigations and/or processing, individuals generally do not have the right or opportunity to object to the collection of this information by the source agencies, nor to the forwarding of the collected information for retention in the NGI and/or the NCIC, nor to the collation of the RISC subset from information in the NGI.").

base.[447] RISC-related information, moreover, is explicitly exempted from individual access, accounting, and amendment provisions in the Privacy Act.[448]

No PIAs have been issued for the other NGI programs, such as Rap Back, the collection of palm prints, or the use of iris technologies. It is thus unclear, on the criminal side, whether the Rap Back program will focus on actual conviction for federal offenses or merely arrest. The civil component is equally undefined and apparently unlimited. Further, it is unclear whether the iris technologies incorporated in the program will be IBI-type iris scans or RBI-type scans. The use of such technologies in a remote manner shifts the discussion to one of investigation and intelligence gathering, raising issues more akin to FRT than to fingerprint or palm print biometrics.

Beyond the above PIAs, it is not known publicly the degree to which the exemptions for classified, sensitive, or private information have prevented further notice of programs underway. In any event, the public's ability to challenge any of the programs thus revealed or to gain further information about their operation is severely limited.

Congress has thus provided the executive with extensive authority to gather personally identifiable information on individuals. Simultaneously, such limits as have been introduced on these authorities appear less than effective with regard to emerging biometric programs. But what about criminal statutes, which regulate the collection of information on individuals in the context of investigation and prosecution—how do these treat emerging biometric programs?

B. CRIMINAL LAW SURVEILLANCE

Strict guidelines limit law enforcement's access to personal information using electronic intercepts. The insertion of a judicial check on the exercise of state authority prior to the collection of data grew directly from circumstances remarkably close to what is being recreated in the realm of RBI—i.e., concern about the use of new technologies to remotely obtain information absent the target's awareness. Existing statutes, however, fail to contemplate the type of technologies driving RBI.

447. *Id.* § 6.4.
448. *Id.* § 7.1.

1. Precursor to Title III: *Katz*, *Berger*, and the Federal Communications Act

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 governs aural surveillance.[449] Congress enacted the statute in response to *Katz v. United States* and *Berger v. New York*, two landmark Fourth Amendment cases, as well as to perceived shortcomings in Section 605 of the Federal Communications Act.[450]

In *Katz*, the petitioner had been convicted of placing a bet from a telephone booth in Los Angeles to bookmakers in Miami and Boston, in violation of a federal statute.[451] At trial, the government introduced evidence derived from a listening device that had been attached to the outside of the phone booth.[452] In a watershed decision authored by Justice Potter Stewart, the Court famously announced that "the Fourth Amendment protects people, not places."[453] In his concurrence, Justice Harlan laid out what has come to be known as the reasonable expectation of privacy test. The test incorporates a subjective element (i.e., that the individual in question exhibit an actual expectation of privacy), as well as an objective element (i.e., that the

449. Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–2522 (2006). For judicial application of Title III to silent video surveillance, see, for example, United States v. Falls, 34 F.3d 674, 680 (8th Cir. 1994) (discussing application of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 to silent video surveillance); United States v. Cuevas-Sanchez, 821 F.2d 248, 251 (5th Cir. 1987) (same); United States v. Biasucci, 786 F.2d 504, 508–09 (2d Cir. 1986) (discussing application of Title III and FISA to silent video surveillance); United States v. Torres, 751 F.2d 875, 880–81 (7th Cir. 1984). *See also* Roberto Iraola, *Lights, Camera, Action!—Surveillance Cameras, Facial Recognition Systems and the Constitution*, 49 LOY. L. REV. 773, 787 n.67 (2003) ("[W]hen the use of video camera surveillance has involved circumstances protected by the Fourth Amendment, some courts have used Title III as a guide for the constitutional standard governing the application for a warrant."); Denise Troy, Comment, *Video Surveillance—Big Brother May Be Watching You*, 21 ARIZ. ST. L.J. 445, 449 (1989) ("Although Title III and the 1986 Act do not include video surveillance, federal courts have borrowed the standards for audio surveillance when reviewing video surveillance orders.").

450. Katz v. United States, 389 U.S. 347 (1967); Berger v. New York, 388 U.S. 41 (1967); *see* People v. Trief, 317 N.Y.S.2d 525, 529–30 n.5 (N.Y. Sup. Ct. 1970), *aff'd*, 323 N.Y.S.2d 659 (N.Y. App. Div. 1971). For a discussion of the shortcomings of the Federal Communications Act of 1934, see *infra* text accompanying notes 463–68.

451. *Katz*, 389 U.S. at 348.

452. *Id.*

453. *Id.* at 351.

expectation be one that society is prepared to recognize as reasonable).[454]

In the second case, *Berger*, the Supreme Court struck down[455] parts of a New York eavesdropping statute, which allowed for the use of an electronic surveillance device for sixty days, with further extensions available without requiring a showing of probable cause.[456] The Court explained:

> The Fourth Amendment commands that a warrant issue not only upon probable cause supported by oath or affirmation, but also "particularly describing the place to be searched, and the persons or things to be seized." New York's statute lacks this particularization . . . . It lays down no requirement for particularity in the warrant as to what specific crime has been or is being committed, nor "the place to be searched," or "the persons or things to be seized" as specifically required by the Fourth Amendment.[457]

The statute in question failed to provide precise and discriminate requirements, making it possible to issue general warrants—instruments roundly rejected at the time of the founding.[458] The New York statute omitted any requirement that the officer engaged in the surveillance believe that an offense had been, or was about to be, committed.[459] It failed to require that the conversations, or property sought, be particularly described.[460] The statute lacked both notice and judicial supervision.[461] This case, along with two cases decided immediately before *Katz*, underscored the importance of the warrant requirement in the Fourth Amendment.[462]

454. *Id.* at 361 (Harlan, J., concurring).

455. *Berger*, 388 U.S. at 44.

456. *Id.* at 43 n.1.

457. *Id.* at 55–56.

458. *Id.* at 58 ("New York's broadside authorization rather than being 'carefully circumscribed' so as to prevent unauthorized invasions of privacy actually permits general searches by electronic devices, the truly offensive character of which was first condemned in *Entick v. Carrington*, 19 How. St. Tr. 1029, and which were then known as 'general warrants.' The use of the latter was a motivating factor behind the Declaration of Independence.").

459. *Id.* at 56.

460. *Id.*

461. *Id.* at 60.

462. *See* Warden v. Hayden, 387 U.S. 294, 301 (1967) (contrasting the Fourth Amendment warrant requirement with the "indiscriminate, general authority" granted to searches in the Colonies); Camara v. Mun. Court, 387 U.S. 523, 528–29 (1967) ("[O]ne governing principle [in Fourth Amendment jurisprudence] . . . has consistently been followed: except in certain carefully defined classes of cases, a search of private property without proper consent is "unreasonable" unless it has been authorized by a valid search warrant."); *see also* David A. Sklansky, Katz v. United States*: The Limits of Aphorism*, *in*

As with the current lack of a statutory regime in regard to RBI, the federal statutes in place at the time of *Berger* and *Katz* proved inadequate in addressing the use of new technologies. The Federal Communications Act provided that "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person."[463] Within three years of the statute's enactment, the Supreme Court fashioned an exclusionary rule to prevent the introduction of illegal wiretap evidence in federal court.[464]

Section 605 of the Federal Communications Act was subject to a number of limitations that significantly undermined its effectiveness. For instance, illegally obtained information could not be introduced into federal court, but it *could* be used in state proceedings.[465] The statute only applied, moreover, to information *actually* introduced into court—it did nothing to regulate the wider problem of wiretapping generally (and subsequent use of such information outside of judicial proceedings).[466] Additionally, the statute *only applied to wire communications*, not to electronic bugs and other forms of eavesdropping.[467] Attorney General Nicholas Katzenback considered it the "worst of all possible solutions."[468] General wiretapping could continue unabated, even as evidence obtained pursuant to probable cause was excluded from court.[469]

2. Title III/Title I

Title III reached beyond Section 605 to govern federal and state officials, as well as private actors.[470] It took the Supreme Court's articulation of Fourth Amendment protections in *Katz* and *Berger* and inserted parallel provisions directly into the law. As originally drafted, however, Title III only applied to

CRIMINAL PROCEDURE STORIES 223 (Carol S. Steiker ed., 2006) (describing the "combined effect" of *Warden*, *Camara*, and other cases).

463. Federal Communications Act of 1934, Pub. L. No. 73-416, § 605, 48 Stat. 1064, 1103 (1934) (codified at 47 U.S.C. § 605 (2006)).

464. Nardone v. United States, 302 U.S. 379, 382 (1937).

465. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 294 (3d ed. 2009).

466. *Id.* at 295.

467. *Id.* at 294.

468. *Id.*

469. *Id.* at 294–95.

470. 18 U.S.C. § 2510 (2006).

wire and oral communications.[471] Eighteen years after its introduction, Congress extended it to apply to a third kind of communication: electronic communications. This legislation, the 1986 Electronic Communications Privacy Act (ECPA), contained three parts which now form the statutory framework for intercepts: the Wiretap Act (Title I of the 1986 act, updating Title III), the Stored Communications Act, and the Pen Register Act.

ECPA understands "wire communications," to which it gives the greatest degree of protection, as

> any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.[472]

An "aural transfer," in turn, is understood as any communication, which, at any point, contains the human voice.[473] It does not need to be a major part of the communication, but merely present, in some form, at some point in the course of the communication.[474] Thus, communications that initially may have included a form of the human voice, but are subsequently translated into codes or tones, still count as aural transfers.[475] The aural transfer must take place, at some point, across a wire or similar medium, although it may be conveyed through air at some point as well.[476]

"Oral communication," which receives slightly less protection, consists of communication "uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation."[477] Such communications generally relate to the use of electronic recording devices, such as bugs.[478]

"Electronic communications" receive the lowest level of protection. They consist of all non-wire and non-oral communi-

471. *Id.* § 2511.
472. *Id.* § 2510(1).
473. *Id.* § 2510(18).
474. *Id.*
475. SOLOVE & SCHWARTZ, *supra* note 465, at 297.
476. *Id.*
477. 18 U.S.C. § 2510(2) (2006).
478. SOLOVE & SCHWARTZ, *supra* note 465, at 297.

cations: i.e., "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[479]

With RBI generally, and FRT more specifically in mind, it is important to underscore again that the *only* types of communications explicitly covered include *wire*, *oral*, and *electronic*. Title III, as amended by Title I of the Electronic Communications Privacy Act, thus *neither explicitly prohibits nor does it, on its face, overtly govern video surveillance*.[480] The Senate Judiciary Committee Report that accompanied the original statute, in reiterating Title III's definition of "aural acquisition" took this one step further, stating "[o]ther forms of surveillance are not within the proposed legislation."[481]

Some judges and legal scholars have suggested that, as a result, Title III/Title I are utterly irrelevant to consideration of video surveillance generally, much less the pairing of video surveillance with facial recognition systems, or the use of video in any sort of biometric identification. Chief Judge Alex Kozinski from the Ninth Circuit Court of Appeals thus asks,

> Does it really follow that, had Congress considered the matter directly, it would have treated video surveillance exactly the same as those methods it did consider? I find it more plausible to infer that by choosing to exclude video surveillance from Title I Congress and the President were recognizing that it is different from wiretapping and should not be treated the same.[482]

In Judge Kozinski's perspective, borrowing elements of Title III/Title I and applying it to video surveillance amounts to legislative drafting—which the court should not be in the business of doing.[483] Instead, in Judge Kozinski's view, the courts are driven back to a Fourth Amendment analysis, outside of statutory considerations.[484]

Other judges, in contrast to Judge Kozinski, recognize the limitations in the statute and its apparent omission of video

479. 18 U.S.C. § 2510(12).

480. *See* SOLOVE & SCHWARTZ, *supra* note 465, at 296 (discussing Title III of the Omnibus Crime Control and Safe Streets Act of 1968).

481. S. REP. NO. 90-1097, at 61 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2178; *see also* United States v. Torres, 751 F.2d 875, 886 (7th Cir. 1984).

482. United States v. Koyomejian, 970 F.2d 536, 545 n.4 (9th Cir. 1992) (Kozinski, J., concurring).

483. *Id.* at 542–45.

484. *Id.* at 542–51; *see also* discussion *infra* Part III (Fourth Amendment considerations).

surveillance, but then nevertheless apply it to this realm.[485] Central here are the statute's procedural protections. In crafting them, Congress drew from the Fourth Amendment discussion in *Katz* and *Berger*.[486]

Under the Wiretap Act, to perform an intercept absent the subject's consent, law enforcement officers must submit an application to a judge detailing the facts relied upon that would justify an intercept order.[487] The officer must demonstrate: probable cause that the target has committed, is committing, or is about to commit an enumerated offense; particularity with regard to the type of crime, location, type of communication to be intercepted, and the identity of the target; necessity (other, less intrusive methods cannot provide the necessary information); and minimization, so as to reduce the acquisition of irrelevant information.[488] In light of the significant amount of information that can be obtained via technology, *these requirements set a higher bar than is otherwise required for a standard search warrant*.

The statute also regulates both who can request the wiretap and how quickly it must be executed. For oral communications, the application must be made by a federal investigative or law enforcement officer with the approval of a high ranking official at the Department of Justice and subsequently signed by a federal judge.[489] The order, in turn, must be executed within thirty days (although an extension is possible).[490]

The statute gives aggrieved targets the ability to challenge the introduction of any wire or oral communication intercepted, or evidence derived therefrom, on the grounds that the communication was unlawfully intercepted, the warrant was insufficient on its face, or the interception was not made in conformity with the order of authorization.[491] In 1984, the Supreme Court carved out a good faith exception: where a law enforcement officer believed a warrant to be valid, the evidence would not be

485. *Koyomejian*, 970 F.2d at 541–42.

486. *See supra* note 450 and accompanying text.

487. 18 U.S.C. § 2518(1)(b) (2006).

488. *Id.* § 2518(3)(a) (probable cause); *id.* § 2518(3)(a), (b), (d),(4)(a)–(e) (particularity); *id.* § 2518(3)(c) (necessity); *id.* § 2518(5) (minimization).

489. *Id.* § 2518(11)(a)(i). Qualified individuals include the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General. *Id.*

490. *Id.* § 2518(5).

491. *Id.* § 2518(10)(a)(i)–(iii).

suppressed.[492] In 1986, Congress amended the statute accordingly.[493] The exclusionary rule contained in the Wiretap Act *does not apply to electronic communications*. Wire or oral communications that fall within the Wiretap Act *are* subject to exclusion, but *not* when they come within the ambit of the Stored Communications Act (which does not have an exclusionary rule).[494] Violations of the Wiretap Act may lead to up to five years imprisonment and a fine of up to $10,000 per violation.[495]

The Wiretap Act contains two important exceptions and a carve-out. First, consent immediately removes a subject from the statute's protections.[496] An individual can therefore record his or her own conversations with others, even without informing others participating in the conversation—and can also allow law enforcement access to the conversation—without falling within the Wiretap Act requirements.[497] A second exception contemplated by the Wiretap Act centers on information obtained in the normal course of business. Communications service providers are allowed "to intercept, disclose, or use" the communication in question "in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service."[498] An additional carve-out limits the reach of the statute. Where criminal activity may be involved, a service provider is authorized to provide intercepted communications to the appropriate authorities.[499]

In contrast to the Wiretap Act, the Stored Communications Act (SCA), as the name suggests, focuses on communications that are not being carried en route but, instead, are being

492. United States v. Leon, 468 U.S. 897, 922–23 (1984).

493. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 101(e), 100 Stat. 1848, 1853 (codified as amended at 18 U.S.C.§ 2518(10)(c)).

494. 18 U.S.C. §§ 2701–2711 (2006).

495. *Id.* §§ 2511(4)(a), 2520(c)(2)(B).

496. *Id.* § 2511(2)(c).

497. It could be argued that the remote collection of biometric information does not involve consent. As is readily acknowledged by the federal agencies using RBI, targets in public spaces may be completely unaware that this information has been recorded, much less used in some way. *See infra* Part III (Fourth Amendment considerations).

498. 18 U.S.C. § 2511(2)(a)(i) (2006).

499. *See id.* § 2511(3)(b)(iv).

stored.[500] This legislation makes it an offense to intentionally access a facility through which electronic communication services are being provided, or access and obtain, alter, or prevent authorized access to wire or electronic communications.[501] Electronic storage is understood in the same way as in the Wiretap Act, i.e., "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof."[502] The violation does not apply to the individual or organization providing the wire or electronic service; however, disclosure of the contents of stored communications by service providers is forbidden.[503] There are a few exceptions to the nondisclosure requirement, one of which relates to providing the information to law enforcement in a criminal law context.[504]

The standards under the SCA are less rigorous than those applied under the Wiretap Act. Less severe criminal penalties apply.[505] There is no exclusionary rule for information illegally obtained.[506] The judicial process, moreover, for obtaining access to stored communications, is less rigorous than the procedure adopted for intercepts under the Wiretap Act. Under the SCA, for information held less than 180 days, the government is required to obtain a warrant supported by probable cause.[507] If the information has been held more than 180 days, the government must merely provide prior notice to the subscriber and obtain an administrative subpoena, a grand jury subpoena, a trial subpoena, or a court order.[508] With subscriber notice, probable cause is not required for the latter; instead, it requires only "specific and articulable facts showing that there are reasonable grounds" to believe communications are relevant to a

500. *Id.* §§ 2701–2711. *See generally* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004) (explaining the basics of the SCA).

501. 18 U.S.C. § 2701(a)(1)–(2) (2006).

502. *Id.* § 2510(17)(A).

503. *Id.* § 2702(a)(1)–(3).

504. *Id.* § 2702(b)(7).

505. *Compare* 18 U.S.C. § 2707 (2006) (SCA penalties), *with id.* §§ 2511(4)(a), 2520(c)(2)(B) (Wiretap Act penalties).

506. *But see id.* § 2707 (setting forth a right to a civil action for equitable relief, damages, and attorney's fees).

507. *Id.* § 2703(a).

508. *Id.* § 2703(b)(1)(A)–(B).

criminal investigation.[509] Absent subscriber notice, however, the government is required to obtain a warrant.[510]

As aforementioned, neither Title III nor the 1986 Electronic Communications Privacy Act specifically addresses video surveillance. A case could be made, however, that where the government intercepts a wire or electronic communication that *includes* video images, such as emailing a video clip from an iPhone or conducting a conversation by webcam, then the Wiretap Act applies. The storage of such information, moreover, would fall within the Stored Communications Act. But it is questionable the extent to which the statutory framework applies to RBI. The actual use of a surveillance camera mounted in a public space does not involve the *interception* of communications (as defined under the Wiretap Act, involving use of a cable or wire).[511] Nor is the act of surveillance indicative of stored communications or images. To the extent that RBI thus depends upon video surveillance for its execution (as, for instance, in some cases of the application of FRT), it does not appear to necessarily come within this regime. To the extent that the surveillance involves the use of audio, it may fall within oral communications, and thus be subject to the Wiretap Act[512]—but here, a question presents itself as to whether individuals, by entering public space, are giving their consent to be observed. Silent video surveillance, in turn, does not appear to be covered.

Importantly, *every* circuit to address silent video surveillance has concluded that Title III/Title I does not apply.[513] Nevertheless, courts look to the standards laid out in Title III/Title I and borrow them for analysis. In other words, Title III/Title I

509. *Id.* § 2703(d). Note that notice can be delayed up to ninety days. *Id.* § 2705(a).

510. *Id.* § 2703(b).

511. *Id.* § 2510(i).

512. *Id.* § 2510(2).

513. United States v. Larios, 593 F.3d 82, 90–91 (1st Cir. 2010); United States v. Falls, 34 F.3d 674, 679–80 (8th Cir. 1994); United States v. Koyomejian, 970 F.2d 536, 538–41 (9th Cir. 1992); United States v. Mesa-Rincon, 911 F.2d 1433, 1436–37 (10th Cir. 1990); United States v. Cuevas-Sanchez, 821 F.2d 248, 251–52 (5th Cir. 1987); United States v. Biasucci, 786 F.2d 504, 508–09 (2d Cir. 1986); United States v. Torres, 751 F.2d 875, 880–81 (7th Cir. 1984); *see* United States v. Ianniello, 621 F. Supp. 1455, 1466–67 (S.D.N.Y. 1985); *In re* Order Authorizing Interception of Oral Commc'ns & Videotape Surveillance, 513 F. Supp. 421, 422–23 (D. Mass. 1980); Sponick v. Detroit Police Dep't, 211 N.W.2d 674, 690 (Mich. Ct. App. 1973); People v. Teicher, 422 N.E.2d 506, 513 (Ct. App. N.Y. 1981).

is seen as providing "guidance in implementing the [F]ourth [A]mendment" in an area[514] not specifically covered by Title I/Title III. Even in circuits where there is pressure not to adopt Title I as the standard, recourse to the statute ensues. The Ninth Circuit, for instance, declined to use every technical requirement of Title I; yet it nevertheless insisted upon the presence of probable cause plus four of the statutory requirements in the Wiretap Act:

> (1) [T]he judge issuing the warrant must find that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous," 18 U.S.C. § 2518(3)(c); (2) the warrant must contain "a particular description of the type of [activity] sought to be [videotaped], and a statement of the particular offense to which it relates," *id.* § 2518(4)(c); (3) the warrant must not allow the period of [surveillance] to be "longer than is necessary to achieve the objective of the authorization, []or in any event longer than thirty days" (though extensions are possible), *id.* § 2518(5); and (4) the warrant must require that the [surveillance] "be conducted in such a way as to minimize the [videotaping] of [activity] not otherwise subject to [surveillance] . . .," [sic] *id.*[515]

These four requirements—those of the best alternative, particularization, limited duration, and minimization—for the Ninth Circuit, "comport with the demands of the Constitution, and guard against unreasonable video searches and seizures."[516] They also reflect the statutory framing put forward in the Wiretap Act.[517]

The statutory framing for criminal law thus fails to account for the types of technologies used in remote biometric identification. But what of the national security realm? Is there a better statutory construction here to which we could turn?

C. NATIONAL SECURITY SURVEILLANCE

The 1978 Foreign Intelligence Surveillance Act provides the principal framework for surveillance conducted under the guise of national security.[518] This statute, and rules subse-

514. *Mesa-Rincon*, 911 F.2d at 1438.

515. *Koyomejian*, 970 F.2d at 542 (additions and omissions in original) (quoting *Cuevas-Sanchez*, 821 F.2d at 252).

516. *Id.*

517. 18 U.S.C. § 2518(3)(A)–(D), (4)(A)–(E), (5) (2006).

518. At the time of the reconciliation debates between the Senate and House bills, the House sought to include language making the Act the "exclusive statutory" means for the Executive to conduct electronic surveillance—implying that the President had inherent surveillance powers outside the statute. The Senate rejected this notion, saying that if the President were to engage in electronic surveillance outside the parameters of FISA, upon judicial

quently implemented by the Foreign Intelligence Surveillance Court, contemplates the use of a range of techniques.[519] It is unclear whether it covers the types of technologies used in remote biometric surveillance. Even if RBI is included as electronic surveillance within the meaning of the statute, restrictions placed on the collection of information within FISA would be difficult to maintain with regard to many of the technologies under development.

1. The Foreign Intelligence Surveillance Act

At the most general level, FISA applies to surveillance conducted in the United States.[520] (Surveillance conducted overseas falls within the President's inherent constitutional authority, as channeled through Executive Order 12333.)[521] The threshold question for FISA thus turns on the Court's Fourth Amendment jurisprudence—i.e., whether the surveillance in question implicates a reasonable expectation of privacy in regard to which a warrant would be required.[522] Part III.B of this Article delves into this question—noting, in the process, that the Fourth Amendment standard applied in national security is significantly weaker than that adopted in the world of criminal law. Assuming, arguendo, that we are within the meaning of

review the Supreme Court should treat the President's actions as consistent with category three of Justice Jackson's concurrence in *Youngstown Sheet & Tube Co. v. Sawyer*: i.e., against the expressed intent of Congress. 343 U.S. 579, 637–38 (1952) (Jackson, J., concurring). The Senate view carried. 124 CONG. REC. 33,787 (1978). Note though that the FISA Amendment Act of 2008 added a new exclusive means provision. *See* FISA Amendments Act of 2008, Pub. L. No. 110-261, § 102, 122 Stat. 2436, 2459 (codified at 50 U.S.C. § 1812).

519. 50 U.S.C. § 1801(f)(1)–(4) (2006 & Supp. IV 2011).

520. *See* 2008 FISA Amendments Act of 2008, Pub. L. No. 110-261, § 101, 122 Stat. 2436, 2448 (codified at 50 U.S.C. § 1812). *But see* 50 U.S.C. § 1801(f)(1) (2006 & Supp. IV 2011) (amending FISA to apply to non-U.S. persons outside the United States in some circumstances).

521. Exec. Order No. 12,333, 46 Fed. Reg. 59,941, 59,941 (Dec. 4, 1981). In limiting FISA to domestic surveillance, Congress did not explicitly authorize the President to conduct surveillance overseas; it simply left the President's consitutional authority unchecked, but also unsupported. *See also* NAT'L SEC. AGENCY, UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE 18, § 4.1(d)(1) (1993) (outlining surveilance authorities relative to the National Security Agency).

522. *See, e.g.*, 50 U.S.C. § 1801(f)(4) (2006 & Supp. IV 2011) ("[T]he installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.").

the Fourth Amendment, however, the central question is whether the techniques employed in remote biometric identification fall within FISA. The answer is far from clear.

FISA, as amended, authorizes the Executive Branch, subject to certain conditions, to collect information on foreign powers and agents of foreign powers, as well as groups "engaged in international terrorism or activities in preparation therefor."[523] Its cornerstone is the definition it adopts of electronic surveillance, understood in two distinct ways. First, as "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication,"[524] and second, as "the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communi-

523. *Id.* § 1801(a)(4). FISA has been amended and its temporary provisions extended by the following instruments: Cable Communications Policy Act of 1984, Pub. L. No. 98-549, § 6(3), 98 Stat. 2779, 2804; Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, §§ 601–603, 112 Stat. 2396, 2404–13 (1998); Intelligence Authorization Act for Fiscal Year 2001, Pub. L. No. 106-567, §§ 602–604, 114 Stat. 2831, 2851–53 (2000); USA PATRIOT Act of 2001, Pub. L. No. 107-56, §§ 901, 1003, 115 Stat. 272, 387, 392; Intelligence Authorization Act for Fiscal Year 2002, Pub. L. No. 107-108, § 314(a), 115 Stat. 1394, 1402 (2001); 21st Century Department of Justice Appropriations Act, Pub. L. No. 107-273, § 305(b), 116 Stat. 1758, 1782 (2002); Homeland Security Act of 2002, Pub. L. No. 107-296, § 898, 116 Stat. 2135, 2258 (2002); Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638; USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, §§ 105–106, 120 Stat. 192, 195–200 (2006); USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, Pub. L. 109-178, §§ 3–4, 120 Stat. 278, 278–81; Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552; FISA Amendments Act of 2008, Pub. L. 110-261, 122 Stat. 2436 (2008); Department of Defense Appropriations Act, 2010, Pub. L. 111-118, 123 Stat. 3409 (2009); An Act to Extend Expiring Provisions of the USA PATRIOT Improvement and Reauthorization Act of 2005 and Intelligence Reform and Terrorism Prevention Act of 2004 until February 28, 2011, Pub. L. No. 111-141, 124 Stat. 37 (2010); FISA Sunsets Extension Act of 2011, Pub. L. 112-3, 125 Stat. 5 (2011); PATRIOT Sunsets Extension Act of 2011, Pub. L. 112-14, 125 Stat. 216 (2011) (extending the temporary provisions until June 1, 2015).

524. 50 U.S.C. § 1801(f)(1) (2006 & Supp. IV 2011); *see also id.* § 1801(f)(2) ("[T]he acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of title 18 . . . ."); *id.* § 1801(f)(3) ("[T]he intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication . . . ."). For the purpose of this discussion, I treat these three definitions under a similar category, as they all deal specifically with wire or radio communications.

cation."[525] RBI technologies do not appear to fall within the first category; they may or may not be currently included in the second.

Central to the concept of electronic surveillance in the first sense is the role of communication—that is, information "sent by or intended to be received by a particular" person.[526] It thus requires the presence of a sender and a receiver. The statute further defines "wire communication" in terms of a common carrier.[527]

Remote biometric identification involves the recording of data—but not in the course of communication. Instead, it creates a record of an individual's physical characteristics, or his or her presence in certain locations or in the proximity of other individuals.[528] It is not limited to communication across a wire, cable or like connection. Even where aural recording may occur in conjunction with biometric identification of two or more persons, such recording takes place *not* by intercepting a communication *while it is being carried by a wire, cable, or other like connection*, but by merely recording an open-air conversation. There is no common carrier involved. RBI therefore does not appear to fall within the current understanding of electronic surveillance in the first sense.[529]

It may, however, fall within the statute's second basic understanding—i.e., the installation or use of a surveillance device used to acquire information other than from a wire or radio communication. What is not clear is whether biometric technol-

525. *Id.* § 1801(f)(4).

526. *Id.* § 1801(f)(1).

527. *Id.* § 1801(*l*) ("[A]ny communication *while it is being carried* by a wire, cable, or other like connection furnished or operated *by any person engaged as a common carrier* in providing or operating such facilities for the transmission of interstate or foreign communications." (emphasis added)). The statute does not define "radio communication." *See id.*

528. 50 U.S.C. § 1861(1) might be read as covering biometric information obtained from private entities. The statute addresses orders for "tangible things (including books, records, papers, documents, and other items)" sought as part of an investigation "to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution." *Id.* Photographs, video, fingerprint, and other data could be considered tangible things under this definition. *See also* USA PATRIOT Act, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 (2001) (replacing former §§ 501–503 in Title V of FISA with new §§ 501–502 of FISA).

529. Similar concerns plague criminal provisions meant to govern surveillance. *See* discussion *supra* Part II.B.

ogies have been included within FISA's remit. Within this broader framing, the statute itself does not limit the types of technologies used.[530] But in 2010, Chief Judge John Bates of the Foreign Intelligence Surveillance Court issued revised *Rules of Procedure*, which specifically addressed new and emerging technologies.[531] The Court currently requires the government to submit a legal memorandum, prior to the use of any new surveillance or search techniques which "(1) explains the technique; (2) describes the circumstances of the likely implementation of the technique; (3) discusses any legal issues apparently raised; and (4) describes the proposed minimization procedures to be applied."[532] The memo must accompany the government's initial application. A separate memorandum must be submitted in support of the government's position on each issue of first impression.[533] The most that could be said here is that it is not clear whether any legal memo has been provided with regard to technologies implicated in remote biometric identification. No information is publicly available one way or the other.

Even if the collection of biometric information falls within the definition of electronic surveillance, a question exists as to whether FISA's other requirements could be met by RBI. Consider, for instance, the statute's strictures with regard to (a) the target of surveillance, (b) the length of the warrant issued by the court, and (c) the statute's minimization requirements.[534] In identifying the target of surveillance, FISA sharply distinguishes between U.S. persons and non-U.S. persons.[535] To engage in surveillance of a U.S. person, there must be probable cause not that the individual engaged, is engaged, or will engage in illegal acts (i.e., the warrant requirement under Title III), but that the individual is a foreign power or an agent thereof.[536] Inclusion as an agent of a foreign power occurs where

530. 50 U.S.C. § 1801 (2006 & Supp. IV 2011).

531. U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT 11 (on file with author).

532. *Id.* 11(b).

533. *Id.* 11(d).

534. 50 U.S.C. § 1802(a)(1) (2006 & Supp. IV 2011).

535. *Id.* § 1801(a).

536. *Id.* § 1802(a)(1). A "foreign power" may be:

> (1) a foreign government or any component thereof, whether or not recognized by the United States; (2) a faction of a foreign nation or nations, not substantially composed of United States persons; (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; (4) a group engaged in international terrorism or activi-

one of two conditions hold: either the target is engaged in espionage and clandestine intelligence activities; or the target is engaged in sabotage or international terrorism.[537] For a non-U.S. person to qualify as an agent of a foreign power, he or she must instead act in the United States as an officer or employee of a foreign power or member of an international terrorist group, conduct clandestine intelligence activities within domestic bounds, or engage in international terrorism or activities in preparation therefor.[538] The duration of the warrant similarly differs based on whether the target is a U.S. person or not. For the former, the period of surveillance is granted up to 90 days.[539] For the latter, the warrant can be extended for up to 120 days, with renewal for a period of up to one year.[540] Minimization, moreover, is only required for information concerning U.S. persons.[541]

While the distinction between U.S. persons and non-U.S. persons, like the distinction between foreign powers and agents thereof, may be sustainable for IBI where the target is limited and specific, it is less applicable to RBI where the indiscriminate scanning of multiple individuals occurs. It may be impossible to know, in a public space, which individuals are U.S. persons and which individuals are not. FRT, iris recognition technology, and other remote technologies serve to identify multiple individuals in crowds—in the process, necessarily scanning *out* some people, even as they help to identify the target. The same difficulties evinced with regard to the target of the surveillance extend to the duration of an order. Admittedly, there is no limit to the number of times a FISA order may be renewed.[542] However, the fact that there is an order, and judicial approval, underscores the distinction. Similarly, which

> ties in preparation therefor; (5) a foreign-based political organization, not substantially composed of United States persons; or (6) an entity that is directed and controlled by a foreign government or governments.

Id. § 1801(a)(1)–(6).

537. A third category, less significant than the first two, includes persons who enter the United States under a false identity. Such U.S. persons must knowingly enter the country under a false identity "for or on behalf of a foreign power or, while in the United States, knowingly assume[] a false or fraudulent identity for or on behalf of a foreign power." *Id*. § 1801(b)(2)(D).

538. *Id.* § 1801(b)(1).

539. *Id.* § 1805(e)(1).

540. *Id.* § 1805(e)(1)–(2).

541. *Id.* § 1801(h)(1).

542. *See id.* § 1805(d)(2).

minimization procedures need to be adopted depends upon being able to distinguish the target—a process that can occur (in the biometrics realm) only after multiple targets have been scanned.

Other requirements in the statute similarly depend upon this distinction. Attorney General certification, for instance, allows the Executive to bypass the Federal Intelligence Surveillance Court (FISC), for one year, where electronic surveillance is directed at communications between foreign powers or from property under their control.[543] In the process, the Attorney General must assert that "no substantial likelihood"[544] exists that a U.S. person will be party to the communications and that every effort will be made to minimize the acquisition, retention, and dissemination of information relating to U.S. persons.[545] In the case of RBI, it is unlikely that that this certification would be sufficient. For information gleaned from public space—particularly within the United States—the likelihood that a U.S. person may be involved may be substantial.

At a more general level, it is worth recognizing that the very nature of RBI runs counter to the specificity that characterizes FISA. The application to FISC for electronic surveillance, for instance, must include either the identity of the target (if known) or a description of the target.[546] It must include a statement of facts supporting the claim that the target is a foreign power (or an agent thereof) and that the facilities to be monitored currently are, or are expected to be, used by a foreign power or its agent.[547] The application must describe the "nature of the information sought and the type of communications or activities to be subjected to the surveillance."[548] A designated national security officer must certify that a significant purpose of the surveillance is to collect foreign intelligence and that "such information cannot reasonably be obtained by normal investigative techniques."[549] The application must specify how the surveillance is to be effected (including whether physical entry is required)[550] and include all previous applications

543. *Id.* § 1802(a)(1)(A)(i)–(ii).
544. *Id.* § 1802(a)(1)(B).
545. *Id.* § 1801(h)(1).
546. *Id.* § 1804(a)(1)–(2).
547. *Id.* § 1804(a)(3)(A)–(B).
548. *Id.* § 1804(a)(5).
549. *Id.* § 1804(a)(6)(c).
550. *Id.* § 1804(a)(7).

involving the "persons, facilities, or places specified in the application," as well as actions taken by the court on these cases.[551] The document includes an estimate of time required for surveillance and requires an explanation why authority should not terminate at the end of the requested period.[552]

What these requirements have in common is that they are specific, targeted, and limited—characteristics more consistent with IBI than with RBI. The act of collecting and storing broad amounts of information on a number of individuals who do not fit the requirements laid out in FISA as targets of surveillance gives rise to concern about whether, and to what degree, remote biometric identification systems could be structured to meet the approach adopted by Congress in passing the statute.

To summarize the statutory inquiry then, Congress has granted the Executive broad authorities to obtain personally identifiable information. While the Privacy Act and the E-Government Act regulate records systems, they contain exceptions within which biometrics systems appear to fall. In the criminal realm, Title III and Title I are looked to for instances of wire, oral, and electronic communications. Yet neither statute directly regulates or prohibits silent video surveillance undertaken for domestic purposes, while questions of consent, an exception in the Wiretap statute, bedevil audio recordings. As for national security surveillance, FISA contemplates the use of electronic surveillance in two primary senses. RBI does not fall subject to the first; it may or may not currently be covered by the second. Even if biometric programs are governed by FISA, there are still significant hurdles to cross with regard to the statute's reliance on distinguishing between U.S. persons and non-U.S. persons—to say nothing of the way in which the specific, limited, targeted nature of FISA runs directly contrary to the types of activities subsumed within RBI. We are thus driven back upon constitutional considerations: specifically, the Fourth Amendment.[553]

551. *Id.* § 1804(a)(8).

552. *Id.* § 1804(a)(9).

553. United States v. Koyomejian, 970 F.2d 536, 541–42 (9th Cir.1992); *see also* United States v. Mesa-Rincon, 911 F.2d 1433, 1436–37 (10th Cir. 1990) ("There must be probable cause supported by an oath or affirmation and a particular description of the place, persons, and things to be searched and seized."); United States v. Cuevas-Sanchez, 821 F.2d 248, 251–52 (5th Cir. 1987) (noting that since Title III does not include video surveillance techniques, the court will turn to the Fourth Amendment for guidance); United States v. Biasucci, 786 F.2d 504, 510 (2d Cir. 1986) ("[T]he *Torres* court bor-

III. FOURTH AMENDMENT CONSIDERATIONS

Despite the direct attack mounted by remote biometric technologies on the core of how we conceive of privacy, Fourth Amendment doctrine provides little by way of relief. Perhaps the most vivid example is the recent decision in *United States v. Jones*,[554] which emphasized the doctrine of trespass—a concept irrelevant for the types of issues that arise with regard to RBI. The Court's treatment of other remote technologies, such as aerial surveillance and thermal imaging, prove similarly inadequate in contemplating the challenge mounted by RBI. The blurring of the line between criminal law and national security, moreover, and the Court's weaker standards in relation to the latter, give rise to further concern.

Sharply increasing this concern are the myriad technologies that are under development but have not yet come of age. That is to say, this Article has thus far addressed what could be considered mainstream biometric technologies with RBI implications, such as facial recognition, iris scanning, fingerprinting, and audio signatures. But what happens when we move into future modalities, such as gait technologies, hormone sniffing, and other signature detection technologies? Hyperspectral imagery, for instance, initially developed for mining and geology, has evolved to encompass applications in both national security and disease surveillance.[555] Like facial recognition, the number of patents being granted in this realm steadily increases.[556] And

rowed four provisions of Title III implementing the Fourth Amendment's requirements of particularity and minimization as a 'measure of the government's constitutional obligation of particular description in using television surveillance to investigate crime.'" (quoting United States v. Torres, 751 F.2d 875, 885 (7th Cir. 1984)); *Torres*, 751 F.2d at 882–86 (stating that Title III has implemented the Fourth Amendment's particularity requirement).

554. United States v. Jones, 132 S. Ct. 945 (2012).

555. *E.g.*, Method & Sys. for Detecting Anomalies in Multispectral and Hyperspectral Imagery Employing the Normal Copositional Model, U.S. Patent No. 7,263,226 col.1 l.30–45 (filed Dec. 4, 2006) (issued Aug. 28, 2007) ("Hyperspectral sensors are a new class of optical sensor that collect a spectrum from each point in a scene. They differ from multi-spectral sensors in that the number of bands is much higher (twenty or more), and the spectral bands are contiguous. For remote sensing applications, they are typically deployed on either aircraft or satellites . . . . Hyperspectral sensors have a wide range of remote sensing applications including: terrain classification, environmental monitoring, agricultural monitoring, geological exploration, and surveillance. They have also been used to create spectral images of biological material for the detection of disease and other applications.").

556. *E.g.*, Adaptive Wavelet Coding of Hyperspectral Imagery, U.S. Patent No. 6,539,122 (filed Mar. 30, 1998) (issued Mar. 25, 2003); Multispectral or

like the other forms of RBI contemplated in this Article, the Court's current jurisprudence has yet to grapple with the consequences, for RBI represents something different in kind—not degree—from what has come before.

A. THE SHADOW MAJORITY IN *UNITED STATES V. JONES*

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[557] In *United States v. Jones*, the Court concluded that the placement of a global positioning device constituted a search within the meaning of the Fourth Amendment.[558] The majority opinion, written by Justice Scalia, zeroed in on the instance of trespass that resulted from the placement of the device on the vehicle itself.[559] Justice Sonia Sotomayor, in her concurrence, did suggest that the Fourth Amendment was concerned with rather more than just "trespassory intrusions on property."[560] She explained, "even in the absence of a trespass, 'a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.'"[561] But, for Justice Sotomayor, "*Katz*'s reasonable-expectation-of-privacy test augmented, but did not displace or diminish, the common-law trespassory test that preceded it."[562] She thus joined the majority on what she considered to be narrower grounds—a sort of constitutional de minimis, which presented itself in the immediate case.

Setting aside the straightforward opinion and concurrence on which the case was decided, it is possible to read *Jones* as a split opinion, or as having what might be considered a shadow majority. Justices Scalia, John Roberts, Anthony Kennedy, Clarence Thomas, and Sotomayor applied the trespassory test

Hyperspectral Imaging Sys. & Method for Tactical Reconnaissance, U.S. Patent No. 6,831,688 (filed Apr. 8, 2002) (issued Dec. 14, 2004); Sys. & Methods for Registering Reflectance and Fluorescence Hyperspectral Imagery, U.S. Patent No. 7,181,055 (filed Aug. 15, 2003) (issued Feb. 20, 2007).

557. U.S. CONST. amend. IV.

558. *Jones*, 132 S. Ct. at 949.

559. *Id.* at 949–54.

560. *Id.* at 954 (Sotomayor, J., concurring).

561. *Id.* at 954–55 (quoting Kyllo v. United States, 533 U.S. 27, 33 (2001)).

562. *Id.* at 955.

without rejecting the reasonable expectation of privacy test.[563] Justices Samuel Alito, Ruth Bader Ginsburg, Stephen Breyer, and Elena Kagan, in turn, adopted a "mosaic" theory,[564] similar to that which was put forward by the D.C. Circuit.[565] Justice Sotomayor did not join Justice Alito's concurrence, precisely because she considered the trespassory test, which established a constitutional minimum, sufficient.[566] In her separate concurrence, however, she went on to endorse the mosaic theory adopted by Justice Alito.[567] She actually went even further, suggesting that in future cases it might be applied more aggressively to technologies not involving trespass.[568]

It could thus be argued that five justices have indicated that a mosaic theory could be applied to future cases involving non-trespassory intrusions. Nevertheless, there is only one true majority position that now forms part of the Court's jurisprudence. This decision squarely centers on trespass. And here, while GPS chips form part of a broader class of surveillance devices that must be physically attached to targets in order to track their movement through public space,[569] not all surveil-

563. *Id.* at 949–54.

564. *See* Orin Kerr, *D.C. Circuit Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, VOLOKH CONSPIRACY (Aug. 6, 2010, 2:46 PM), http://www.volokh.com/2010/08/06/d-c-circuit-introduces-mosaic-theory-of-fourth-amendment-holds-gps-monitoring-a-fourth-amendment-search.

565. *Compare* United States v. Maynard, 615 F.3d 544, 558–66 (D.C. Cir. 2010) (arguing that the government's constant GPS surveillance of defendant's whereabouts for twenty-eight days amounted to a search under the Fourth Amendment), *with Jones*, 132 S. Ct. at 964 (Alito, J., concurring) ("In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.").

566. *Jones*, 132 S. Ct. at 954–55 (Sotomayor, J., concurring).

567. *See id.* at 955 (expressing agreement with Justice Alito that long-term GPS surveillance violates reasonable expectations of privacy).

568. *See* discussion *infra* accompanying notes 731–33.

569. GPS, which originated as a network of twenty-four satellites, was launched by the U.S. Department of Defense for military applications. *What Is GPS?*, GARMIN, http://www8.garmin.com/aboutGPS (last visited Nov. 2, 2012). Since it was extended to civilian applications and updated to reflect new technological breakthroughs, GPS receivers use the satellites to triangulate their position on earth—some with an accuracy of within fifteen meters. *Id*. Also included in this category are battery-operated devices (a.k.a. "beepers") which emit signals that can be picked up via radio frequencies. 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.7(e) (4th ed. 2011). Law enforcement uses of beepers, particularly in the realm of drug enforcement, involve attaching a device to individuals or goods and then using

lance devices involve the same element of contact.[570] Factory-installed devices in cars or GPS chips in cell phones may prove equally sufficient for transmitting the car's whereabouts. As Justice Sotomayor noted, "In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance."[571] Biometric collection devices like cameras and video feeds enabled with facial recognition technology, or remote iris scanners, involve no physical touching.[572] For these, a more appropriate framing might therefore be the test developed under *Katz*. Indeed, this was the position Justice Sotomayor took in *Jones*.[573] Yet the application of this test in considering the advent of other remote technologies has yielded a body of jurisprudence that proves similarly inadequate for contemplating the challenges faced with regard to RBI.

B. PUBLIC VERSUS PRIVATE SPACE: AERIAL SURVEILLANCE AND THERMAL IMAGING

Remote biometrics represents a new and emerging field, which the Court has yet to confront. There are other technologies that give rise to parallel considerations. The Court has here applied the reasonable expectation of privacy test to areas such as aerial surveillance and thermal imaging, in the process drawing a distinction between public and private space. In this construction, however, *looser* standards apply to the former—which is precisely the domain of interest with regard to RBI. Yet it is this sphere which gives rise to some of the greatest privacy concerns as RBI represents something different in kind—not degree—to what has come before.

In *United States v. Knotts*, an opinion authored by (then) Justice William Rehnquist, the Court held that monitoring the signal of a beeper placed in a container of chemicals en route to a cabin did not invade the cabin owner's legitimate expectation of privacy.[574] The Court grounded its decision in *Katz*: "A person traveling in an automobile on public thoroughfares has no rea-

a receiver to monitor the target's movement. *Id.*

570. *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring); *id.* at 961 (Alito, J., concurring).

571. *Id.* at 955 (Sotomayor, J., concurring).

572. Note, however, with regard to iris scans, an argument could be marshaled that physical penetration of the body occurs.

573. *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).

574. United States v. Knotts, 460 U.S. 276, 285 (1983).

sonable expectation of privacy in his movements from one place to another."[575] The Court pointed to the diminished expectation of privacy that derived from the function of the object of surveillance: i.e., transportation as opposed to one's residence or "the repository of personal effects."[576]

An automobile, the Court suggested, "has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view."[577] Thus, while the respondent, as the owner of the cabin, had an expectation of privacy within his dwelling place, "no such expectation extended to the visual observation of [his] car arriving on his premises after leaving the public highway"[578]—nor did it extend to the movement of the container of chemicals outside the cabin in the open fields.[579] Similarly, again on the grounds of public versus private space, in *United States v. Karo*, the Court found that a beeper entering the home constituted a search within the meaning of the Fourth Amendment.[580]

The Court has adopted a consistent approach in its treatment of other, emerging remote technologies, such as aerial surveillance and thermal imaging. Consider first aerial surveillance. The so-called naked eye doctrine suggests that flying a plane or a helicopter over an individual's backyard does not constitute a search within the meaning of the Fourth Amendment.[581] In *California v. Ciraolo*, the Court thus held that any member of the public flying 1000 feet above a home could observe the same information that any police officer could observe.[582] Aerial observation of the curtilage, however, *could* become invasive, "either due to physical intrusiveness or through modern technology which discloses to the senses those intimate associations, objects or activities otherwise imperceptible to police or fellow citizens."[583] The Supreme Court subsequently con-

575. *Id.* at 281.

576. *Id.* (quoting Cardwell v. Lewis, 417 U.S. 583, 590 (1974)).

577. *Id.*

578. *Id.* at 282.

579. *Id*. *Knotts* centered on a combination of visual surveillance and limited electronic monitoring of a vehicle. It left open the warrantless, extensive use of a GPS chip to electronically monitor the totality of a target's movements over time. *See id*. at 284–85.

580. United States v. Karo, 468 U.S. 705, 714–15 (1984).

581. California v. Ciraolo, 476 U.S. 207, 213–15 (1986).

582. *Id.* at 215.

583. *Id.* at 215 n.3 (quoting Brief for Petitioner at 14–15, California v. Ciraolo, 476 U.S. 207 (1986) (No. 84-1513)).

sidered a helicopter flying 400 feet above the ground. In *Florida v. Riley*, the Court held that neither the home over which the helicopter flew, nor the curtilage, was protected from an inspection that involved no physical invasion.[584] Again, the public versus private distinction prevailed.

Similarly, the Court has held that taking aerial photographs of an industrial complex does not constitute a search within the meaning of the Fourth Amendment.[585] In *Dow Chemical Co. v. United States*, the Court determined that manufacturing plants were different in kind from what happens within the curtilage of a home.[586] The industrial nature of the fixtures to be surveyed in this context more closely resembled an open field than the privacy of a dwelling.[587] In *Dow Chemical*, moreover, a standard map-making camera had been used, a technology that could not see through walls.[588] The Court was careful to note that the pictures did not reveal any identifiable human faces.[589] The Court suggested, "[a]n electronic device to penetrate walls or windows so as to hear and record confidential discussions . . . would raise very different and far more serious questions."[590]

In *United States v. Jackson*, the Tenth Circuit later relied on *Katz*, *Ciraolo*, and *Dow Chemical* in holding that video cameras installed on telephone poles, capable of observing "only what any passerby would easily have been able to observe," did *not* fall within a Fourth Amendment definition of privacy.[591]

From these cases, we can conclude that the reasonable expectation of privacy depends, at the most general level, on the nature of the location under surveillance. That is, surveillance inside a home is given a much higher degree of protection than surveillance of public space. Indeed, in *United States v. Nerber*, a hidden video camera was used to film a narcotics transaction in a motel room.[592] After the informants left, the camera was left running, and over the next three hours, recorded illegal ac-

584. Florida v. Riley, 488 U.S. 445, 451–52 (1989).
585. Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986).
586. *Id.*
587. *Id.* at 236–37.
588. *Id.* at 229.
589. *Id.* at 238 n.5.
590. *Id.* at 239.
591. United States v. Jackson, 213 F.3d 1269, 1281 (10th Cir. 2000), *vacated*, 531 U.S. 1033 (2000).
592. United States v. Nerber, 222 F.3d 597, 599 (9th Cir. 2000).

tivity.[593] The government conceded, and the court agreed, that the audio surveillance conducted after they left the motel room was inadmissible under Title III.[594] But as far as the silent video recording was concerned, the court held that "considering the totality of the circumstances of this case, including but not limited to the nature of the governmental intrusion" the defendants had a reasonable expectation of privacy that they would not be subject to video surveillance once the informants left.[595] The expectation of privacy in a motel room was impacted by the nature of the intrusion. Both of these elements, the place and the nature of the intrusion, thus need to be taken into account.

Other technologies have pressed this point even further.[596] Consider thermal imaging: even if physical intrusion within the home does not occur, and sensory enhancing technologies are used to glean information about what happens inside the home, the higher expectation of privacy that accompanies domestic dwellings may give rise to a search within the meaning of the Fourth Amendment. The key case here is *Kyllo v. United States*,[597] which centered on detecting home-grown marijuana. The Supreme Court, in an opinion authored by Justice Scalia, held that the use of sense-enhancing technology to obtain information about the interior of the home, which could not have been obtained without physical intrusion into that protected area, constituted a search within the meaning of the Fourth Amendment.[598]

In *Kyllo*, the fact that the thermal surveillance device was not in general public use was relevant.[599] This suggests that the technology itself, and the ubiquitous nature of the technology, may have an effect on an individual's expectation of privacy. If this is the test for RBI, though, then it is at least probative that the commercial sector is largely unregulated with regard to its use of biometric identification. It is, moreover, already taking concrete steps to yield a profit from its use and clearly interest-

593. *Id.*

594. *Id.* at 604–05.

595. *Id.* at 600.

596. *See, e.g.*, Kevin Gordon, *Automatic License Plate Recognition*, L. & ORD., May 2006, at 10, 10 (2006) (describing technology that scans license plates and automatically checks them against law enforcement databases).

597. Kyllo v. United States, 533 U.S. 27 (2001).

598. *Id.* at 34–35.

599. *Id.* at 40.

ed in developing further in this direction. A few examples will suffice.

PittPatt, developed at Carnegie Mellon (and subsequently bought by Google), is just one of many off-the-shelf technologies that can identify individuals in photographs, matching them with other images found online and then joining the images with other personally identifiable information found on the Internet.[600] Facebook operates similar software, called Face.com, which automatically identifies individuals in pictures uploaded to the site and inquires whether users would like to tag the photos accordingly.[601] Viewdle's Social Camera, in turn, uses advanced technology to detect and tag photos.[602] Currently in its beta version, the application (developed for Android phones) tags pictures based on FRT and then allows them to be synced and shared through Facebook, Flickr, MMS, or e-mail, automatically tying the images to individual contact information already stored in the phone.[603] In 2010, Apple acquired Polar Rose, a company specializing in FRT.[604] RecognizeMe is an iPhone app that allows for phones to be unlocked by facial scanning.[605]

Private use of FRT, paired with video technology extends into public space. The Venetian hotel in Las Vegas, for instance, has now rolled out billboards that draw on the technology to advertise bars, clubs, and restaurants appropriate for

600. John Paul Titlow, *As Facial Recognition Improves, New Privacy Controversies Await*, READWRITEWEB (Oct. 7, 2011), http://www.readwriteweb.com/archives/facial_recognition_privacy_concerns.php. Somewhat disconcertingly, this technology may allow users to predict individuals' Social Security numbers using Facebook profile information such as date of birth. Mello, *supra* note 265.

601. Titlow, *supra* note 600; *see also* Daniela Minicucci, *Face and Iris Recognition Apps Both Thrilling and Threatening*, GLOBAL NEWS, Sept. 28, 2011, http://www.globalnews.ca/technology/6442491279/story.html.

602. Minicucci, *supra* note 601.

603. *Id*.

604. Titlow, *supra* note 600.

605. This app was billed as "[t]he ONLY Facial Recognition app on App Store," "[t]he Most Popular & Astonishing app," and "[o]ne of the TOP Apps of 2011." *Recognize Me 1.0*, QARCHIVE, http://recognize-me.by-best-apps-and-games.qarchive.org (last visited Nov. 2, 2012); *see also* Oliver Haslam, *RecognizeMe Brings Biometric Facial Recognition Security for Unlocking iPhone [Cydia Tweak]*, REDMOND PIE, May 18, 2011, http://www.redmondpie.com/recognizeme-brings-biometric-facial-recognition-security-for-unlocking-iphone-cydia-tweak.

the demographic identified.[606] In Chicago, a startup called SceneTap, links FRT to cameras located in dance clubs and bars, allowing users to determine the best male to female ratios before choosing their destinations.[607] Adidas and Intel are working together to install digital walls in stores, with plans to target passers-by with shoe displays appropriate to their age and gender.[608] In 2011, Kraft demonstrated a "Meal Planning Solution" kiosk at the National Retail Federation Show, featuring the use of FRT to determine which products to advertise to consumers as they peruse the aisles in grocery stores.[609] Privacy advocates worry not just about such FRT usages, but the pairing of it to Facebook. In such instances, there would be substantially less guesswork: instead of assuming, for instance, that women between certain ages were more likely to have children at home, it could simply check the user's Facebook account and find out precisely what ages the children were and what their interests might be.[610] This would allow companies like Kraft to market their products directly to consumers as they enter into stores—based on remote biometric technologies.

C. ELIMINATION OF THE DISTINCTION BETWEEN CRIMINAL LAW AND NATIONAL SECURITY

A further consideration in the Court's Fourth Amendment jurisprudence is its traditional reliance on the distinction between criminal law and national security. Two observations here are of note: first, the standards applied to the latter are considerably weaker than those adopted in the former realm.

606. John Eggerton, *Rockefeller Seeks FTC Report on Face Recognition and Privacy*, BROADCASTING & CABLE, Oct. 19, 2011, 5:06 PM, http://www.broadcastingcable.com/article/475505-Rockefeller_Seeks_FTC_Report_On_Face_Recognition_And_Privacy.php; Shan Li & David Sarno, *Advertisers Start Using Facial Recognition to Tailor Pitches*, L.A. TIMES, Aug. 21, 2011, http://articles.latimes.com/2011/aug/21/business/la-fi-facial-recognition-20110821.

607. Mello, *supra* note 265.

608. Li & Sarno, *supra* note 606.

609. Julia Carpenter, *Matching Moms with Macaroni: New Kraft Kiosks Scan Your Face to Recommend Recipes*, N.Y. DAILY NEWS, Jan. 18, 2011, http://articles.nydailynews.com/2011-01-18/news/27087917_1_kiosk-new-kraft-recipe-ideas; Linda Tischler, *Kraft Store Kiosk Scans Your Face Then Knows What to Feed It [Video]*, FAST COMPANY (Jan. 14, 2011), http://www.fastcompany.com/1716684/kraft-store-kiosk-scans-your-face-then-knows-what-feed-it-video.

610. Kashmir Hill, *Kraft to Use Facial Recognition Software to Give You Macaroni Recipes*, FORBES (Sept. 1, 2011, 11:14 AM), http://www.forbes.com/sites/kashmirhill/2011/09/01/kraft-to-use-facial-recognition-technology-to-give-you-macaroni-recipes.

Second, as a matter of both law and policy, the lines between these areas are becoming increasingly blurred.

1. Fourth Amendment Standards with Regard to National Security

In 1967, *Katz* dealt with the attachment of a device to the outside of a telephone booth.[611] The Court, considering new technologies in the context of electronic surveillance, adopted a doctrine based on the reasonable expectation of privacy for criminal activity—but it did not settle the question of what to do when national security matters were on the line.[612] Justice Byron White, in his concurrence, emphasized that the presumption against warrantless searches *could* be overcome by pressing need: "We should not require the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable."[613] Justice White's words pointed to a different set of rules: under some circumstances, requirements otherwise applicable within criminal law might alter.

Justice William Douglas, joined by Justice William Brennan, strongly objected to Justice White's assertion and pointed out a certain conflict of interest: "Neither the President nor the Attorney General is a magistrate. In matters where they believe national security may be involved they are not detached, disinterested, and neutral as a court or magistrate must be."[614] The constitutional responsibility of the Executive is to "vigorously investigate and prevent breaches of national security and prosecute those who violate the pertinent federal laws."[615] Justice Douglas concluded,

> Since spies and saboteurs are as entitled to the protection of the Fourth Amendment as suspected gamblers like petitioner, I cannot agree that where spies and saboteurs are involved adequate protection of Fourth Amendment rights is assured when the President and Attorney General assume both the position of adversary-and-prosecutor and disinterested, neutral magistrate.[616]

611. Katz v. United States, 389 U.S. 347, 348 (1967).
612. *Id.* at 358 n.23.
613. *Id.* at 364 (White, J., concurring).
614. *Id.* at 359 (Douglas, J., concurring).
615. *Id.* at 359–60.
616. *Id.* at 360.

The national security issue proved contentious, and a de facto double standard evolved. Physical surveillance and electronic bugging became subject to the reasonable expectation of privacy test, discussed above. But wiretapping, and surveillance where national security might be involved, constituted a different sort of a question because, there, looser considerations might satisfy constitutional demands. President Lyndon Johnson explained in his 1967 State of the Union: "We should protect what Justice Brandeis called the 'right most valued by civilized men'—the right to privacy. We should outlaw all wiretapping—public and private—wherever and whenever it occurs, *except when the security of this Nation itself is at stake . . . .*"[617]

The Executive thus carved out a special sphere for national security surveillance, independent of criminal law standards with regard to Fourth Amendment jurisprudence. Title III, introduced the following year, focused on criminal law. In enacting the statute, *Congress specifically exempted national security*—leaving such investigations in the hands of the executive branch.[618]

In 1972, a landmark decision further addressed the question of the Fourth Amendment in the context of national security. In *United States v. U.S. District Court (Keith),* the Supreme Court held 8-0 that Title III did *not* authorize the Executive to engage in electronic surveillance for national security purposes;

617. President Lyndon Johnson, State of the Union Address (Jan. 10, 1967) (emphasis added), *available at* http://www.presidency.ucsb.edu/ws/index.php?pid=28338.

618. Omnibus Crime Control Act and Safe Streets Act of 1968, Pub. L. No. 90-351, § 802, 82 Stat. 197, 212 (codified as amended at 18 U.S.C. § 2511(3)) ("Nothing contained in this chapter or in section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. *Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government.* The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power." (emphasis added)).

rather, it simply reflected congressional neutrality.[619] For the Court, warrantless domestic wiretapping for national security did not fall exclusively within the constitutional remit of the Executive.[620] While the duty of the state to protect itself has to be weighed against "the potential danger posed by unreasonable surveillance to individual privacy,"[621] such "Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch."[622]

Justice Lewis Powell, writing for the majority, recognized that executive officers could hardly be regarded as neutral and disinterested: "Their duty and responsibility are to enforce the laws, to investigate, and to prosecute. . . . [T]hose charged with this . . . duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks."[623] He highlighted the dangers: "[U]nreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech."[624] Domestic security surveillance thus did *not* fall under one of the exceptions to the warrant requirement under the Fourth Amendment.[625] Justice Powell rejected the government's suggestion that national security matters are "too subtle and complex for judicial evaluation."[626] Nor did he accept that "prior judicial approval will fracture the secrecy essential to official intelligence gathering."[627] The former would suggest that such surveillance might not be warranted in the first place; the second had long been an aspect of ordinary criminal activity.

The Executive Branch largely ignored this decision.[628] Under the guise of national security, the FBI, National Security Agency (NSA), CIA, and DoD continued to operate domestic

619. 407 U.S. 297, 308 (1972). This case is known as *Keith*, in accordance with the name of the district court judge who initially ordered the government to release a number of illegally-obtained conversations.

620. *See id*. at 316 (stating that "Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch").

621. *Id.* at 314–15.

622. *Id.* at 316–17.

623. *Id.* at 317 (citation omitted).

624. *Id.*

625. *Id.* at 320.

626. *Id.*

627. *Id.*

628. *See* LAURA K. DONOHUE, THE COST OF COUNTERTERRORISM 222 (2008).

surveillance programs, many of which came to light in the course of the Church Hearings.[629] Like many of the biometric programs discussed in Part I, above, each of these surveillance efforts began as a limited inquiry but "gradually extended to capture more information from a broader range of individuals and organizations."[630]

The Executive responded to the public outcry that followed the Church Committee's findings with a series of actions to curb surveillance in the national security realm. In 1976, President Gerald Ford banned the NSA from intercepting telegraphs and forbade the CIA from conducting electronic or physical surveillance of U.S. citizens.[631] Clarence Kelly, whom President Richard Nixon had nominated to take over the FBI following J. Edgar Hoover's death in 1972, publicly apologized for the Hoover era.[632] Significant gaps, however, continued to exist. For example, while the Privacy Act ostensibly regulated the collection, maintenance, use, and dissemination of citizens' personal data,[633] as discussed in Part II *supra*, it also provided certain exemptions for the CIA.[634] National security information held by any agency came to be exempted from certain requirements.[635]

Congress thus came to the 1978 Foreign Intelligence Surveillance Act with the aim of addressing national security surveillance. The law, as discussed in Part II *supra*, limits the statute to foreign powers and to agents of foreign powers—including groups "engaged in international terrorism or activities in preparation therefor."[636] While the previous discussion of FISA focused on the type of surveillance being undertaken, the relationship of the statute to the Court's Fourth Amendment jurisprudence is no less probative of the failure of the legislature or the judiciary to take account of the unique challenges of RBI.

629. *See id*.

630. *Id.* at 223.

631. GEOFFREY R. STONE, PERILOUS TIMES: FROM THE SEDITION ACT OF 1798 TO THE WAR ON TERRORISM 496 (2004).

632. *Id.*

633. 5 U.S.C. § 552a (2006).

634. GINA MARIE STEVENS, CONG. RESEARCH SERV., RL 31730, PRIVACY: TOTAL INFORMATION AWARENESS PROGRAMS AND RELATED INFORMATION ACCESS, COLLECTION, AND PROTECTION LAWS 6 (2003).

635. *Id.*

636. 50 U.S.C. § 1801(a)(4) (2006).

The reasonable expectation of privacy test is built directly into FISA's definition of electronic surveillance.[637] The level of probable cause needed, however, for an order to issue departs from that required for a warrant within criminal law.[638] This change reflected Justice Powell's position in *Keith*:[639]

> Given . . . potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. *Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens.* For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection.[640]

Under Title III, the court must find "on the basis of the facts submitted by the applicant that . . . there is probable cause for belief that an individual is committing, has committed, or is about to commit" an enumerated offense.[641] In contrast, FISA

637. *See id.* § 1801(f)(1), (3), (4) ("(1) [T]he acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, *under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes* . . . (3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, *under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes* . . . (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, *under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes*." (emphasis added)).

638. *See* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 318–19 (1972).

639. Note that while the Court in *Keith* emphasized that the case related to *domestic* security, rather than *foreign* security, the distinction quickly fell by the wayside.

640. *Keith*, 407 U.S. at 322–23 (emphasis added). Justice Powell continued:

> It may be that Congress, for example, would judge that the application and affidavit showing probable cause need not follow the exact requirements of § 2518 but should allege other circumstances more appropriate to domestic security cases; that the request for prior court authorization could, in sensitive cases, be made to any member of a specially designated court . . . and that the time and reporting requirements need not be so strict as those in § 2518.

Id. at 323.

641. 18 U.S.C. § 2518(3)(a) (2006). For wire and oral communications (e.g., telephone and microphone interceptions), § 2516(1) enumerates a long list of predicate offenses that range from bank fraud, *see id.* § 1344, to unlawful pos-

does not always require a showing of an imminent crime, or the elements of a specific offense. Instead, it requires the court to find "on the basis of the facts submitted by the applicant" that "there is probable cause to believe that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power."[642]

FISA defines the phrases "foreign power" and "agent of a foreign power" in a manner that may (or may not) require a showing of criminal conduct. Five of its seven definitions of criminal conduct can be satisfied without any showing of criminal activity.[643] The fourth definition, which refers to "international terrorism," does require some level of criminal conduct. The term incorporates, inter alia, "activities that . . . involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State."[644] An organization *may* be a "foreign power" under the fourth definition when it engages in "activities in preparation" for international terrorism—a standard which may (or may not) be more expansive than criminal law, in which a substantial step towards completing the crime generally constitutes attempt.[645]

For a U.S. person to be included as an agent of a foreign power,[646] in turn, one of two conditions must hold: either the

session of a firearm, *see id.* § 922(g), and including espionage, *see, e.g.*, *id.* § 794 (2006), assassination, *see, e.g.*, *id.* §§ 351, 1751, sabotage, *e.g.*, *id.* § 2155, terrorism, *see e.g.*, *id.* § 2332, and aircraft piracy, *see* 49 U.S.C. § 46502. 18 U.S.C. § 2518(1). For electronic communications (e.g., electronic mail or facsimile messages under Title III), any federal felony may serve as a predicate. *Id.* § 2516(3) (2006).

642. 50 U.S.C. § 1805(a)(3) (2006 & Supp. III 2008); *see also id.* § 1805(b) (requiring probable cause that the facilities to are to be used by a foreign power or an agent thereof).

643. *See id.* § 1801(a) (defining foreign power as (1) a foreign government or any component thereof, whether or not recognized by the United States; (2) a faction of a foreign nation or nations, not substantially composed of United States persons; (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; (4) a group engaged in international terrorism or activities in preparation therefor; (5) a foreign-based political organization, not substantially composed of United States persons; (6) an entity that is directed and controlled by a foreign government or governments; (7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction).

644. *Id.* § 1801(c).

645. *See id.* § 1801(a)(4).

646. The statute defines "agent of a foreign power" as

target is engaged in espionage and clandestine intelligence activities or the target is engaged in sabotage or international terrorism.[647] (A third category, less significant than the first two, includes persons who enter the United States under a false identity.)[648] For the first of these categories, an individual engaged in clandestine intelligence activities on behalf of a foreign power may qualify as an agent only where such actions "involve," "may involve" or "are about to involve" a "violation of the criminal statutes of the United States."[649] This standard falls short of what would otherwise be constitutionally required in criminal law.

In other words, special rules apply for national security. Clandestine intelligence activities require *something less than probable cause* for evidence of criminal activity.[650] For sabotage or international terrorism, the standard is closer to the criminal norm.[651] For foreign powers, no criminal standard applies.[652]

The Court has roundly rejected efforts to challenge the constitutional sufficiency of FISA's provisions on Fourth

> any person who—(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States; (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States; (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power; (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or (E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

Id. § 1801(b)(2).

647. *Compare id.* (establishing the definition of "agent of a foreign power" that applies to all persons), *with id.* § 1801(b)(1) (establishing the definition of "agent of a foreign power" that applies to any person other than a United States person).

648. For fraudulent identity, a U.S. person must knowingly enter the country under a false identity "for or on behalf of a foreign power or, while in the United States, knowingly assume[] a false or fraudulent identity for or on behalf of a foreign power." *Id.* § 1801(b)(2)(D). As a practical matter, it could be argued that some crime will occur in conjunction with such designation, but probable cause does not need to be demonstrated up front.

649. *Id.* § 1801(b)(2)(A).

650. *See id.*

651. *See id.* § 1801(b)(2)(C).

652. *See id.* § 1801(a).

Amendment grounds (as well as Fifth Amendment due process grounds) because of the purpose for which the statute was created: securing foreign intelligence information.[653] That is to say, the lesser probable cause standards in FISA meet the requirements of the Fourth Amendment, *precisely because of the aims of the statute itself*. In *United States v. Cavanagh*, the Ninth Circuit explained,

> It is true . . . that the [FISA] application need not state that the surveillance is likely to uncover evidence of a crime; but as the purpose of the surveillance is not to ferret out criminal activity but rather to gather intelligence, such a requirement would be illogical. *See United States District Court*, 407 U.S. at 322 . . . (recognizing distinction between surveillance for national security purposes and surveillance of "'ordinary crime'") . . . . [T]here is no merit to the contention that he is entitled to suppression simply because evidence of his criminal conduct was discovered incidentally as the result of an intelligence surveillance not supported by probable cause of criminal activity.[654]

In *Keith*, Justice Powell suggested that the legislative branch could make finer distinctions than the judiciary in the context of national security.[655] The Supreme Court has since endorsed this approach by rejecting petitions for certiorari challenging FISA.[656] And the Executive has made considerable use of its authorities under the statute. Thus, the three branches appear to have reached agreement: a different constitutional standard applies in the realm of national security.

The electronic surveillance provisions of FISA that might apply to the acquisition of RBI have not remained static. The 2008 FISA Amendments Act (FAA) broadened the risk of inter-

653. *See, e.g.*, United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987); United States v. Ott, 827 F.2d 473, 476–77 (9th Cir. 1987); United States v. Megahey, 553 F. Supp. 1180, 1185–93 (E.D.N.Y. 1982), *aff'd without opinion*, 729 F.2d 1444 (2d Cir. 1983), *re-aff'd post-trial sub nom.* United States v. Duggan, 743 F.2d 59 (2d Cir. 1984), *superseded by statute*, USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 271, *as recognized in* United States v. Abu-Jihaad, 630 F.3d 102 (2d Cir. 2010).

654. United States v. Cavanagh, 807 F.2d 787, 790–91 (9th Cir. 1987).

655. *See* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 323–24 (1972).

656. *See, e.g.*, United States v. Squillacote, 532 U.S. 971, 971 (2001) (denying certiorari). The government purportedly subjected the petitioners to 550 consecutive days of round-the-clock telephone and physical surveillance under FISA, in the course of which the government intercepted/transcribed several psychotherapy suggestions, later using the information to "exploit" one of the petitioner's psychiatric vulnerabilities. Petition for Writ of Certiorari at 1, *Squillacote*, 532 U.S. 971 (No. 00-969). The court of appeals found that the government had made a sufficient showing to warrant FISA surveillance without, though, giving the defense counsel any opportunity to examine or challenge the government's submissions in support of its FISA authority. *Id*.

ception, lowering the government's burden for demonstrating probable cause and reducing FISC's oversight abilities.[657] The Court has yet to determine the constitutionality of these weaker standards under the Fourth Amendment.

Prior to the FAA, the statute required the government to identify the specific targets of surveillance.[658] The court then had to find probable cause that the target was a foreign power or agent thereof and using (or about to use) the facility to be monitored.[659] Under the FAA, FISC now need only determine that the general procedures to be followed comply with the subsections of the statute and with the Fourth Amendment—meaning that the probable cause determination is no longer particularized for non-U.S. persons believed to be outside the United States.[660] The legislation absolves the Attorney General and Director of National Intelligence of providing the identity of specific targets; instead, they must simply submit a written document, certifying that the targets are not within domestic bounds.[661] FISC's analysis must only consider the government's general procedures.[662]

Following enactment of the statute, the ACLU filed a suit challenging the FAA on both Fourth and First Amendment grounds. The Southern District of New York dismissed the claim on the grounds that the plaintiff could not demonstrate standing.[663] In March 2011, a three-judge panel of the Second Circuit Court of Appeals unanimously reversed the case, allowing it to proceed.[664] An effort to send the case for rehearing en banc failed in September 2011, allowing the challenge to move forward.[665] The case, formerly *Amnesty v. McConnell*, then *Amnesty v. Blair*, and now *Amnesty v. Clapper* (in keeping with successive Directors of National Intelligence), challenged the

657. *See* Amnesty Int'l USA v. Clapper, 638 F.3d 118, 125–26 (2d Cir. 2011).

658. *See id.*

659. *See id.* at 126.

660. *See* 50 U.S.C. § 1881a(i)(3)(A) (2006 & Supp. IV 2011).

661. *See id.* § 1881a(g)(2)(A)(i)(I).

662. Amnesty Int'l USA v. Clapper, 667 F.3d 163, 166 (2d Cir. 2011) (Lynch, J., concurring in the denial of rehearing en banc).

663. Amnesty Int'l USA v. McConnell, 646 F. Supp. 2d 633, 635 (S.D.N.Y. 2009), *vacated sub nom.* Amnesty Int'l USA v. Clapper, 638 F.3d 118, 150 (2d Cir. 2011), *reh'g en banc denied*, *Amnesty Int'l USA*, 667 F.3d at 164.

664. *Amnesty Int'l USA*, 638 F.3d 118 (2d Cir. 2011) *reh'g en banc denied*, 667 F.3d at 164.

665. *Amnesty Int'l USA*, 667 F.3d at 164.

constitutionality of the new sections of the statute, which authorized "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[666] In February 2012, the Obama Administration filed a petition for certiorari, which the Court granted.[667] Argument was heard on October 29, 2012.[668]

666. 50 U.S.C. § 1881(a) (2006 & Supp. IV 2011).

667. Petition for Writ of Certiorari, Clapper v. Amnesty Int'l USA, No. 11-1025 (filed Feb. 2012).

668. *Docket No. 11-1025*, SUP. CT. U.S., http://www.supremecourt.gov/Search.aspx?FileName=/docketfiles/11-1025.htm (last visited Nov. 2, 2012). It is worth noting here that the question of whether litigants have standing is an important one for consideration of surveillance programs generally and, as such, one that inevitably accompanies the use of RBI for national security purposes. Efforts to bring suit in similar contexts, based on a generalized challenge to gathering intelligence, have fallen rather short. In *United Presbyterian Church v. Reagan*, for example, the D.C. Circuit considered a suit lodged against the President and the heads of various agencies, questioning the legality of Executive Order 12333. 738 F.2d 1375, 1377 (D.C. Cir. 1984); *see* U.S. Intelligence Activities, Exec. Order No. 12333, 46 Fed. Reg. 59,941 (Dec. 4, 1981), *reprinted as amended in* 50 U.S.C. § 401 (2006). Appellants challenged the instrument on Fourth Amendment grounds (protection against unreasonable searches and seizures), as well as the First and Fifth Amendments. *United Presbyterian*, 738 F.2d at 1377. The claim cited the immediate threat of being targeted for surveillance as depriving the appellants of their legal rights. *Id*. The Court of Appeals for the D.C. Circuit found the alleged grievances

> insufficient to satisfy the injury-in-fact standing requirement imposed by Article III of the Constitution. "[A]t an irreducible minimum, Art. III requires the party who invokes the court's authority to 'show that he personally has suffered some actual or threatened injury as a result of the putatively illegal conduct of the defendant.'" *Valley Forge Christian College v. Americans United for Separation of Church & State, Inc.*, 454 U.S. 464, 472, (1982), *quoting Gladstone, Realtors v. Village of Bellwood*, 441 U.S. 91, 99 (1979). The injury or threat must be "distinct and palpable," *Warth v. Seldin*, 422 U.S. 490, 501 (1975), "concrete," *Schlesinger v. Reservists Committee to Stop the War*, 418 U.S. 208, 221 (1974), "direct," *O'Shea v. Littleton*, 414 U.S. 488, 494 (1974), *quoting Massachusetts v. Mellon*, 262 U.S. 447, 488 (1923), and "both 'real and immediate,' not 'conjectural' or 'hypothetical,'" *id.*, *quoting Golden v. Zwickler*, 394 U.S. 103, 109–10 (1969), and *United Public Workers v. Mitchell*, 330 U.S. 75, 90 (1947).

United Presbyterian, 738 F.2d at 1378.

A similar challenge emerged in *American Civil Liberties Union v. National Security Agency*, which addressed the constitutionality of the National Security Agency's warrantless wiretap program, believed at the time to be targeting individuals understood to be in contact with al Qaeda. 493 F.3d 644, 648–49 (6th Cir. 2007). The plaintiffs in the case included the ACLU, the Council on American-Islamic Relations, the National Association of Criminal Defense Lawyers, and Greenpeace, along with five authors and journalists, all of whom had previously communicated with people in or from the Middle East. District Court Judge Anna Diggs Taylor, the first to encounter the case, considered the program to be a violation of the Fourth Amendment. According to

2. Blurring of the Lines

The weaker Fourth Amendment standards that apply in the realm of national security become more pressing when one considers the gradual breakdown of the distinction between criminal law and national security. Dual-use authorities, dual-use institutions, and new institutional relationships are contributing to this phenomenon, in the process transgressing important barriers.

Consider FISA. Post-9/11, Congress amended the legislation to allow it to be applied, under certain circumstances, to criminal investigations. The Foreign Intelligence Surveillance Court of Review initially embraced the alterations, suggesting broad agreement between all three branches of government. What these changes suggest is that, at times, biometric surveillance used for criminal purposes may fall within a less rights-protective, national security framing.

Prior to the 9/11 attacks, a wall had been erected between intelligence and law enforcement. The USA PATRIOT Act, however, changed the gathering of foreign intelligence from

the judge, the purpose of the Fourth Amendment was precisely "to assure that Executive abuses of the power to search would not continue in our new nation." Am. Civil Liberties Union v. Nat'l Sec. Agency, 438 F. Supp. 2d 754, 774 (E.D. Mich. 2006), *vacated*, 493 F.3d 644 (6th Cir. 2007). Judge Taylor quoted Justice Stewart's opinion in *Katz v. United States*: "'Over and again this Court has emphasized that the mandate of the (Fourth) Amendment requires adherence to judicial processes' (citation omitted) and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." *Id.* at 774–75 (quoting Katz v. United States 389, U.S. 347, 357 (1967)). *Keith*, Judge Taylor noted, recognized that the clause did not assume executive officers were neutral and disinterested parties to disputes. *Id.* at 775 (citing United States v. Dist. Court (*Keith*), 407 U.S. 297, 317 (1972)). According to Judge Taylor, the Fourth Amendment "requires reasonableness in all searches. It also requires prior warrants for any reasonable search, based upon prior-existing probable cause, as well as particularity as to persons, places, and things, and the interposition of a neutral magistrate between Executive branch enforcement officers and citizens." *Id.* However much Congress conceded to the Executive in enacting FISA (such as allowing for delayed warrant applications in exigent circumstances, providing for a single, specialized court, or extending the duration of approved wiretaps from 30 days (under Title III) to 90 days), the Executive had overstepped its authority in running the warrantless program and, in the process, had violated the Fourth Amendment. *Id.* at 781–82. The Sixth Circuit Court of Appeals overturned Judge Taylor's decision. The ruling turned on standing. *Am. Civil Liberties Union*, 493 F.3d at 648. In February 2008, the Supreme Court denied certiorari, ending any chance of the lawsuit moving forward. Am. Civil Liberties Union v. Nat'l Sec. Agency, 552 U.S. 1179, 1179 (2008) (denying certiorari).

"the" sole reason for surveillance, to merely a "significant" purpose.[669] Attorney General John Ashcroft quickly seized on this power and issued guidelines that said such authorization could be sought even if the primary ends of the surveillance related to ordinary crime.[670] These guidelines collapsed the wall between the FBI's prosecution and intelligence functions.

Although the FISC had functioned secretly for nearly three decades, in May 2002 it published an opinion for the first time to protest the guidelines.[671] The court required that the wall be re-built. FISC centered its directive on the statutory minimization requirement and raised concerns about abuse.[672] The court recognized the reasons a wall had been placed between intelligence gathering and criminal investigations and suggested that "[t]he 2002 procedures appear to be designed to . . . substitute the FISA for Title III electronic surveillances and Rule 41 searches."[673] By removing the wall,

> criminal prosecutors will tell the FBI when to use FISA (perhaps when they lack probable cause for a Title III electronic surveillance), what techniques to use, what information to look for, what information to keep as evidence and when use of FISA can cease because there is enough evidence to arrest and prosecute.[674]

Such measures did not appear to be reasonably designed "to obtain, produce, or disseminate foreign intelligence information."[675] And so, the court imposed conditions.

For the first time in the history of FISC, the government appealed.[676] The Executive argued that Congress's intent in

669. USA PATRIOT Act, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291 (2001); *see also id.* § 201, 115 Stat. at 278 (expanding the Attorney General's authority to conduct wire taps to obtain information about terrorism-related crimes); *id.* § 207, 115 Stat. at 282 (expanding FISA authority with respect to duration of surveillance orders).

670. Memorandum from John Ashcroft, Att'y Gen., to Dir. of the Fed. Bureau of Investigation; Assistant Attorney Gen., Criminal Div., Counsel for Intelligence Policy & U.S. Attorneys (Mar. 6, 2002), *available at* http://www.fas.org/irp/agency/doj/fisa/ag030602.html ("[The USA PATRIOT Act] allows FISA to be used *primarily* for a law enforcement purpose, as long as a significant foreign intelligence purpose remains." (emphasis in original)).

671. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 621 (FISA Ct. 2002).

672. It noted, for instance, that in September 2000, the government had admitted that it had made "misstatements and omissions of material facts" in seventy-five of its FISA applications. *Id.* at 620.

673. *Id.* at 623.

674. *Id.* at 624.

675. *Id.* at 625 (quoting 50 U.S.C. §§ 1801(h)(1); 1821(4)(A)).

676. *In re* Sealed Case, 310 F.3d 717, 717 (FISA Ct. Rev. 2002).

changing the wording from "the" to "a significant" purpose was, precisely, to eliminate the wall between intelligence and law enforcement agencies.[677] The attempt to impose minimization standards was so intrusive as to "exceed the constitutional authority of Article III judges."[678]

Six months later, a three-judge appellate court, appointed by Chief Justice William Rehnquist, issued its first opinion reversing the lower court's ruling.[679] The appellate court suggested that FISA was never meant to apply only to foreign intelligence information relative to national security, but that it could also be used for ordinary criminal cases.[680] The court went even further: it interpreted the USA PATRIOT Act to mean that the *primary* purpose of the investigation could, indeed, be criminal investigations, "[s]o long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution."[681] Stopping a conspiracy, for instance, would suffice.[682]

This change suggests that for the collection of biometric data as an aspect of foreign intelligence surveillance, at least insofar as RBI uses new and emerging technologies (such as FRT) to track individuals through public space, a FISA framing—with weaker standards than apply in criminal law—might apply, even when the primary aim of the investigation is criminal in nature.

Paralleling the shift to dual-use authorities is the creation and expansion of dual-use institutions which are responsible for matters related to criminal law and national security. The

677. *Id.* at 732.

678. *Id.* at 722.

679. *Id.* at 746.

680. *Id.* at 727.

681. *Id.* at 735.

682. *Id.* To reach this conclusion, the appellate court rejected the Fourth Circuit court's finding in *United States v. Truong*, 629 F.2d 908 (4th Cir. 1980), a case that rejected warrantless search and surveillance once a case crossed into a criminal investigation. *In re Sealed Case*, 310 F.3d at 725–26. The Fourth Circuit held that the "Executive Branch need not always obtain a warrant for foreign intelligence surveillance," but that the Executive should be excused from obtaining a warrant only where surveillance was conducted "primarily" for foreign intelligence purposes. *Truong*, 629 F.2d at 913. This became the "primary purpose" test for FISA, which has since been followed by other courts of appeals. *See In re Sealed Case*, 310 F.3d at 726. The appeals court suggested that *Truong* may even have been at fault for contributing "to the FBI missing opportunities to anticipate the September 11, 2001 attacks," and added that "special needs" may provide further justification for departing from constitutional limits. *Id.* at 744–45.

FBI, for instance, functions as both a law enforcement organization and an intelligence agency.[683] Over the past decade, there have been increasing efforts to construct procedures within the FBI which, as an operational matter, run the gamut. In September 2008, for example, Attorney General Mukasey issued new rules for domestic FBI operations.[684] The goal was to standardize criminal, national security, and foreign intelligence investigative activities—i.e., to ensure the same approval, notification, and reporting requirements.[685] The new rules recognized four broad authorities granted to the FBI: (1) to collect domestic and foreign intelligence and conduct investigations to detect, obtain information about, and prevent and protect against federal crimes and threats to the national security; (2)

683. It is the lead agency for the investigation of all crimes for which DOJ has primary or concurrent jurisdiction and which involve terrorism within the United States' statutory jurisdiction. *See, e.g.*, FED. BUREAU OF INVESTIGATION, THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC OPERATIONS 5 (Sept. 2008) [hereinafter AGG-DOM], *available at* http://www.justice.gov/ag/readingroom/guidelines.pdf. Terrorism is defined as "the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." 28 C.F.R. § 0.85(*l*) (2012). Similarly, the term "[f]ederal crime of terrorism" is defined as an offense (1) "calculated to influence or affect the conduct of government by intimidation or coercion, or to retaliate against government conduct," 18 U.S.C. § 2332b(g)(5)(A) (2006), and (2) is a violation of federal statutes related to, among others, the "destruction of aircraft or aircraft facilities," *id.* § 2332b(g)(5)(B)(i); *see id.* § 32, "violence at international airports," *id.* § 2332b(g)(5)(B)(i); *see id.* § 37, or "arson within special maritime and territorial jurisdiction" of the United States, *id.* § 2332b(g)(5)(B)(i); *see id.* § 81.

684. AGG-DOM, *supra* note 683. The document replaced previous guidelines, which had been introduced between 1976 and 2006. The AGG-DOM replaced: (1) *The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations* (May 30, 2002); (2) *The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection* (Oct. 31, 2003); (3) *The Attorney General's Supplemental Guidelines for Collection, Retention, and Dissemination of Foreign Intelligence* (Nov. 29, 2006); (4) *The Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, Counterintelligence or International Terrorism Intelligence Investigations* (Aug. 8, 1988); and (5) *The Attorney General's Guidelines for Reporting on Civil Disorders and Demonstrations Involving a Federal Interest* (Apr. 5, 1976). AGG-DOM, *supra* note 683, at 14; *see also* FED. BUREAU OF INVESTIGATION, DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE xi (Dec. 16, 2008) [hereinafter DIOG], *available at* https://www.eff.org/sites/default/files/filenode/FBI_guidelines/domestic_investigations_and_operations_guide_part1.pdf (revising the FBI's internal policies to implement the AGG-DOM).

685. DIOG, *supra* note 684, at 1; *see also* AGG-DOM, *supra* note 683, at 5–11.

to provide investigative assistance to other federal, state, local, or tribal agencies, and certain foreign agencies; (3) to conduct intelligence analysis and planning; and (4) to retain and share information.[686]

DHS and other agencies, like the FBI, consider their responsibilities to extend from criminal law to national security.[687] Such institutional emphases similarly reflect in dual-use programs and systems. The FBI's Next Generation Identification, for instance, incorporates databases that extend from pedophiles to "known or suspected terrorists."[688]

New institutional relationships further contribute to the breakdown of barriers between criminal law and national security. Interoperability, in turn, is beginning to alter traditional institutional relationships, with federal—and federalist—implications. Efforts to create common platforms, to ensure consistent collection of information, and to allow agencies access to other agencies' data erodes important protections—which is, of course, the aim. Such initiatives may take the form of common standards, memoranda of understanding, the creation of new (joint biometrics) agencies and institutions, or the formation of new networks (such as the Joint Terrorism Task Forces).[689] Each of these allows agencies to gain access to information to which it would not otherwise be privy, either because of bureaucratic divisions at the federal level, or because of local/state primacy in regard to criminal law. To the extent that data procurement and analysis reaches into intelligence gathering, the blending of these worlds carry Fourth Amendment implications, lowering the standards that might otherwise be applied in criminal law.[690]

686. DIOG, *supra* note 684, at 3 (also noting that each of these must be conducted consistent with the DIOG, as well as the AGG-DOM).

687. *See* GOV'T ACCOUNTABILITY OFFICE, GAO-03-715T, HOMELAND SECURITY: INFORMATION SHARING RESPONSIBILITIES, CHALLENGES, AND KEY MANAGEMENT ISSUES 1–2 (2003), *available at* http://www.gao.gov/assets/110/109951.pdf.

688. NEXT GENERATION IDENTIFICATION, *supra* note 201.

689. *Protecting America from Terrorist Attack: Our Joint Terrorism Task Forces*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/investigate/terrorism/terrorism_jttfs (last visited Nov. 2, 2012).

690. An additional consideration not addressed in the text is the point at which analysis becomes a search. That is, the collection of information may be understood as falling outside of the contours of that search, but the analysis of this same information may then move the discussion into the search domain. Similarly, the collection of urine may not itself be a search, but urinalysis may then be deemed to fall within its contours. *See generally* Nat'l Treasury Emps.

D. DEGREE OF INTRUSIVENESS

Why does it matter? Why should the Executive's sudden expansion into this realm, the lack of a statutory framing, and the inadequacy of Fourth Amendment doctrine in the face of remote biometric identification give us pause? The reason is because the technologies at issue in RBI present a unique challenge to liberty. The level of intrusiveness represents something different in kind—not degree—from what has come before. It alters the type of surveillance that can occur. It allows for prolonged surveillance to an extent not previously contemplated. And it carries significantly fewer resource limitations than might otherwise accompany individual search or identification, allowing for significantly greater occurrence of both.

1. Type and Kind of Surveillance

Since the onset of the digital revolution, courts have recognized the considerable power derived from the use of electronic technologies. In the 1973 case of *United States v. King,* for instance, the Ninth Circuit recognized that Title III's procedures "were designed to protect the general public from abuse of the awesome power of electronic surveillance."[691] In *Torres*, the Seventh Circuit suggested that "[t]elevision surveillance is identical *in its indiscriminate character* to wiretapping and bugging. It is even more invasive of privacy, just as a strip search is more invasive than a pat-down search."[692] The Tenth Circuit agreed that "video surveillance can be vastly more intrusive" than audio surveillance.[693]

As different technologies combine, the level of intrusiveness may significantly deepen. Thus, Judge Richard Posner recognized in *Torres*, "[w]e think it is . . . unarguable that television surveillance is exceedingly intrusive, especially in combination . . . with audio surveillance, and inherently indiscrim-

Union v. Von Raab, 489 U.S. 656, 665 (1989) (holding that the urinalysis test required as part of the U.S. Customs' Service drug-screening program constitutes a search and is therefore subject to Fourth Amendment analysis); Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 617 (1988) (holding that state-compelled collection and testing of urine constitutes a search under the Fourth Amendment).

691. United States v. King, 478 F.2d 494, 505 (9th Cir. 1973).

692. United States v. Torres, 751 F.2d 875, 885 (7th Cir. 1984).

693. United States v. Mesa-Rincon, 911 F.2d 1433, 1437 (10th Cir. 1990).

inate, and that it could be grossly abused—to eliminate personal privacy as understood in modern Western nations."[694]

Adding biometric recognition technology presumably takes us further down the path. No longer are we discussing merely audio or video surveillance. Nor is the information gleaned limited to physical movement of vehicles through space. Instead, we are considering personally identifiable information, the loss of anonymity, social association, the attribution of actions to individuals, and the possibility of serializing this information to generate new knowledge in the process. The difference is not merely one of degree—which is how, thus far, the Court has been considering parallel technologies.

Consider here continual surveillance using GPS devices—a realm at least comparable to video surveillance paired with facial recognition in the tracking thereby made possible. In *Knotts*, Justice Rehnquist, writing for the Court, suggested that the augmentation of human sensory faculties by science and technology does not create a new category in terms of Fourth Amendment protections. "Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case."[695] Following a car through public space using a beeper, therefore, did not constitute a search.[696]

To the extent that beepers or GPS merely augment law enforcement's senses, creating a more efficient system, the difference may indeed be, more narrowly, one of degree.[697] Accordingly, Judge Posner argued in *United States v. Garcia* that the only difference between the police following a car around and

694. *Torres*, 751 F.2d at 882.

695. United States v. Knotts, 460 U.S. 276, 282 (1983).

696. *Id.* at 278, 285. The Court left open whether the act of installing a device in a vehicle converts the tracking into a search. *Id.* at 279 n.*. *See also* United States v. Karo, 468 U.S. 705, 713–14 (1984) (noting that monitoring a beeper is "less intrusive than a full-scale search," but that it allows the Government to obtain information it could not have otherwise learned without a warrant); United States v. Garcia, 474 F.3d 994, 996–97 (7th Cir. 2007) (noting that the courts of appeals have been divided on the question of whether installing a beeper turned a tracking into a search).

697. *See, e.g.*, United States v. Hufford, 539 F.2d 32, 34 (9th Cir. 1976), *partially overruled by* Jones v. United States, 132 S. Ct. 945 (2012), *as recognized in* United States v. Pineda-Moreno, 688 F.3d 1087 (9th Cir. 2012); United States v. Frazier, 538 F.2d 1322, 1326 (8th Cir. 1976) (Ross, J., concurring); Dunivant v. State, 273 S.E.2d 621, 625 (Ga. Ct. App. 1980) (comparing binoculars to beepers).

observing the car's movements via cameras mounted on lampposts or satellite imaging was one of technology, with no meaningful Fourth Amendment implications.[698] For Judge Posner, GPS devices, technologically on the side of surveillance cameras or satellite imagery, do not constitute a search under the Fourth Amendment.[699]

Not everyone agrees. On the other side stands the argument that, even in relation to GPS, the reason for using the technology in the first place is because *it allows law enforcement to do something that it otherwise could not accomplish*. Such technologies therefore represent something different in kind, not merely degree, from physical surveillance.[700] The First Circuit explained:

> Use of a beeper to monitor a vehicle involves something more . . . than magnification of the observer's senses as in the use of a helicopter, binoculars, radar, or the like. Whether or not the beeper is legally implanted by use of stealth or attached by a technical trespass to the vehicle, it transforms the vehicle, unknown to its owner, into a messenger in the service of those watching it. While a driver has no claim to be free from observation while driving in public, he properly can expect not to be carrying around an uninvited device that continuously signals his presence.[701]

What amounted to efficiency, then, for Judge Posner, added up to a significant increase in the intrusiveness of the surveillance for the First Circuit.

Judge Posner did recognize that there were limits to his position. One significant difference for him, between the police officer following the car around and using video, satellite, or GPS technologies, was the potential for "wholesale surveillance."[702] He wrote:

> It would be premature to rule that such a program of mass surveillance could not possibly raise a question under the Fourth Amendment—that it could not be a search because it would merely be an efficient alternative to hiring another 10 million police officers to tail every vehicle on the nation's roads.[703]

Efficiency halted at the doorstep of mass surveillance. The *Garcia* case did not address the precise contours of where such a

698. *Garcia*, 474 F.3d at 997–98.

699. *Id.* at 997.

700. United States v. Holmes, 521 F.2d 859, 866 n.13 (5th Cir. 1975), *aff'd en banc*, 537 F.2d 227 (5th Cir. 1976) ("If this be true . . . then there is no need for the device in the first place. Its value lies in its ability to convey information not otherwise available to the government.").

701. United States v. Moore, 562 F.2d 106, 112 (1st Cir. 1977).

702. *Garcia*, 474 F.3d at 997–98.

703. *Id.* at 998.

line might be drawn. Nor did Judge Posner consider whether and what type of restrictions might be constitutionally required.

Applied to RBI, one could convincingly argue that biometric technologies so change the parameters as to make the use of this technology different in kind.[704] As Christopher Milligan observes, most people do not expect that their actions in public will be randomly observed, with a host of private data simultaneously linked to them.[705] This suggests an expectation of anonymity and personal privacy, even when standing in a crowd in the public sphere. Consistent with this view, courts have recognized the right to various forms of anonymity, suggesting the existence of, at a minimum a "quasi-right" in anonymity—protected in some cases, but not in others.[706] To the extent that RBI technology takes this away, it is different in kind than the sort of targeted identification activity contemplated by fingerprint and palm biometrics.

The absence of individualized suspicion in particular changes the context. Suspicionless searches have been accepted by the courts in other areas. In *National Treasury Employees Union v. Von Raab*, for instance, the Court allowed for federal employees as a whole to be scanned for drug use, even when no individual was directly suspected of using drugs.[707] Similarly, *Michigan Department of State Police v. Sitz* allowed

704. *See*, e.g., Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1392–98 (2004); John J. Brogan, *Facing the Music: The Dubious Constitutionality of Facial Recognition Technology*, 25 HASTINGS COMM. & ENT. L.J. 65, 81–82 (2002); Max Guirguis, *Electronic Visual Surveillance and the Reasonable Expectation of Privacy*, 9 J. TECH. L. & POL'Y 143, 168–71 (2004); Christopher S. Milligan, Note, *Facial Recognition Technology, Video Surveillance, and Privacy*, 9 S. CAL. INTERDISC. L.J. 295, 319–20 (1999); Carla Scherr, Note, *You Better Watch Out, You Better Not Frown, New Video Surveillance Techniques are Already in Town (and Other Public Spaces)*, 3 I/S: J. L. & POL'Y FOR INFO. SOC'Y 499, 500 (2008); Robert H. Thornburg, Note, *Face Recognition Technology: The Potential Orwellian Implications and Constitutionality of Current Uses Under the Fourth Amendment*, 20 J. MARSHALL J. COMPUTER & INFO. L. 321, 330–31 (2002).

705. Milligan, *supra* note 704, at 318–19.

706. Alexander T. Nguyen, Note, *Here's Looking at You, Kid: Has Face-Recognition Technology Completely Outflanked the Fourth Amendment?*, 7 VA. J.L. & TECH. 2, para. 52 (2002) (citing Ohio v. Akron Ctr. for Reprod. Health, 497 U.S. 502 (1990); Fla. Star v. B.J.F., 491 U.S. 524 (1989); Hazelwood Sch. Dist. v. Kuhlmeier, 484 U.S. 260 (1988); United States v. Brown, 250 F.3d 907 (5th Cir. 2001); Roe v. Aware Woman Ctr. for Choice, Inc., 253 F.3d 678 (11th Cir. 2001)).

707. Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656 (1989).

suspicionless searches for DUI-related checkpoints.[708] But in the realm of RBI, suspicionless searches would result in at least four significant changes that shift the nature of what is being considered.

First, massive amounts of contextual data would be captured. Carla Scherr explains:

> Unlike the beat cop, automated video surveillance sees everything, forgets nothing, and never gets tired or distracted. It captures digital images that can be viewed at any time, from any place, as many times as desired, and can be modified and used well beyond the original intent of either the image collector or the subject. The extreme zoom capabilities of today's cameras allow them to be so distant from the subject that the subject is likely to be unaware and unsuspecting that surveillance might be present, and the camera can capture a subject's image at a level of intimacy that would be totally unacceptable if the image were observed in person. Not even the cover of darkness provides protection; images can be captured in very low lighting and can capture information, such as the subject's temperature, that is not apparent to the naked eye.[709]

Second, the incident would re-create the conditions of a consensual encounter—without carrying any of the consensuality otherwise involved. Third, the information thus obtained could be linked with other data, generating new knowledge in the process. Fourth, such data could retroactively implicate individuals in a way significantly different from immediate drug testing might reveal. There is something at least odd about having the definition of a search depend upon information not available at the time the search occurs.

2. Length of Surveillance

Along with a shift in the type and kind of surveillance under consideration, the expansion to RBI introduces the potential for prolonged surveillance. In *Maynard*, as aforementioned, the District of Columbia Circuit Court examined the question left open in *Knotts*: whether extended surveillance using a GPS device to track an individual constituted a search within the meaning of the Fourth Amendment.[710] The court found that "unlike one's movements during a single journey, the whole of

708. Mich. Dep't of State Police v. Sitz, 496 U.S. 444 (1990).

709. Scherr, *supra* note 704, at 505–06 (citations omitted).

710. United States v. Maynard, 615 F.3d 544, 563–64 (D.C. Cir. 2010), *aff'd sub nom.*, United States v. Jones, 132 S. Ct. 945 (2012); *see also* United States v. Marquez, 605 F.3d 604, 609–10 (8th Cir. 2010); United States v. Pineda-Moreno, 591 F.3d 1212, 1216–17 (9th Cir. 2010); United States v. Garcia, 474 F.3d 994, 996–98 (7th Cir. 2007) (expressly reserving the question of whether wholesale or mass electronic surveillance requires a warrant).

one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all of those movements is effectively nil."[711] In considering whether something was exposed to the public, the question for the court is not what another person could physically or lawfully do, but rather what a reasonable person would expect others to do.[712]

This approach reflected the Court's jurisprudence in similar contexts. In *Florida v. Riley*, for instance, Justice Sandra Day O'Connor, whose concurrence was integral to the judgment, noted:

> Ciraolo's expectation of privacy was unreasonable not because the airplane was operating where it had a "right to be," but because public air travel at 1,000 feet is a sufficiently routine part of modern life that it is unreasonable for persons on the ground to expect that their curtilage will not be observed from the air at that altitude.[713]

In *Bond v. United States*, the Supreme Court reaffirmed this approach.[714] The Court did not focus on what the passengers *could* have done but instead on what a reasonable passenger *would expect*.[715] *Kyllo* picked up on this line of reasoning as well, where the question became whether the technology in question was in general use.[716] In *Maynard*, the court explained:

> It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's hitherto private routine.[717]

Although the government did not argue that constructive exposure derived from the fact that the individual's movements at the time were in full public view, the court nevertheless addressed it: "When it comes to privacy . . . precedent suggests that the whole may be more revealing than the parts. Applying that precedent to the circumstances of this case, we hold the information the police discovered using the GPS device was not

711. *Maynard*, 615 F.3d at 558.
712. *Id.* at 559.
713. Florida v. Riley, 488 U.S. 445, 453 (1989) (O'Connor, J., concurring).
714. Bond v. United States, 529 U.S. 334, 338 (2000).
715. *Id.* at 338–39.
716. Kyllo v. United States, 533 U.S. 27, 34 (2001).
717. 615 F.3d at 560.

constructively exposed."[718] The court recognized that, similar to the mosaic theory applied in the state's secrets realm, bits of information that may initially appear unimportant change in quality when given a broader context.[719]

Prolonged surveillance, for the court, thus revealed a different sort of information than that obtained by short-term surveillance. Repeatedly going to the gym or attending a synagogue tells a different story than just visiting those places one time. Such sequences reveal more information. Thus, a single trip to an OBGYN is simply one data point. But followed a week later by a visit to Babies"R"Us, a different picture may emerge.[720] The court noted that a reasonable person does not expect that everything she does will be recorded.[721] Instead, there is a basic expectation of anonymity.[722] The court thus concluded that the object of the prolonged surveillance in the case, Jones, not only had an expectation of privacy, but that it was reasonable.[723]

The court of appeals denied a petition for rehearing en banc.[724] Chief Judge David Sentelle, joined by Judges Karen Henderson, Janice Rogers Brown, and Brett Kavanaugh, dissented.[725] Judge Sentelle, offering a different-in-kind analysis, pointed out that the GPS device merely enhanced human senses.[726] The case was therefore undistinguishable from *Knotts*.[727] The volume of information obtained, over time, mattered not at all: "The fact that no particular individual sees . . . all [an individual does over the course of a month] does not make the

718. *Id.* at 560–61; *see also id.* at 562 ("The difference is not one of degree but of kind, for no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life, nor the departure from a routine that, like the dog that did not bark in the Sherlock Holmes story, may reveal even more.").

719. *Id.* at 562.

720. *Id.*

721. *Id.* at 563.

722. *Id.*

723. *Id.* at 566. ("This case does not require us to, and therefore we do not, decide whether a hypothetical instance of prolonged visual surveillance would be a search subject to the warrant requirement of the Fourth Amendment.").

724. United States v. Jones, 625 F.3d 766, 767 (D.C. Cir. 2010).

725. *Id.*

726. *Id.* at 768.

727. He stated, "There is no material difference between tracking the movements of the *Knotts* defendant with a beeper and tracking [respondent] with a GPS." *Id.* at 768.

movements any less public."[728] He flatly rejected the argument "that [the] whole reveals more . . . than does the sum of its parts."[729] As the court concluded in *Knotts*, "[t]he reasonable expectation of privacy as to a person's movements on the highway is . . . zero. The sum of an infinite number of zero-value parts is also zero."[730]

In *United States v. Jones*, even as she joined the majority on grounds of trespass, Justice Sotomayor picked up on this line of reasoning, suggesting that "[i]n cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention."[731] She continued,

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. See, [sic] *e.g., People v. Weaver*, 12 N.Y. 3d 433, 441–42, 909 N.E. 2d 1195, 1199 (2009) ("Disclosed in [GPS] data. . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on"). The Government can store such records and efficiently mine them for information years into the future. And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices. . . .[732]

Justice Sotomayor's words suggested perhaps an even more aggressive posture than that adopted by Justice Alito in his concurrence.[733]

What animates these judicial decisions is a growing uneasiness about whether the information generated by certain forms of surveillance is different in kind, or merely degree, from what could otherwise be gleaned. The prolonged nature of the surveillance, along with its perfect recall, here plays an important role. Even where these arguments have surfaced, the technologies in question have been less intrusive than that which marks the biometric realm. A GPS chip may reveal

728. *Id.*

729. *Id.* at 769.

730. *Id.*

731. United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring).

732. *Id.* at 955–56 (citation omitted).

733. *See id.* at 961 (Alito, J., concurring) (discussing the problems of long-term GPS surveillance).

where the car goes, but the verification of personally identifiable information, which is at issue in remote biometric identification, is more invasive in its direct and personal link to a specific individual.

To the extent that the information gleaned is understood as third party data, the Court's jurisprudence presents further difficulties. The Supreme Court has made it clear that information voluntarily provided to third parties does not fall subject to any reasonable expectation of privacy.[734] The federal government, however, is designing systems specifically to gather third party biometric data, such as pictures from social networking sites, CCTV footage, and images provided by friends and relatives.[735] This information can then be paired with biographic information—i.e., hard data about what an individual does or says, where they live, what they buy, and with whom they associate. In the aggregate, such information could provide a staggering amount of insight into a target's life. As Justice Sotomayor notes in *Jones*, the third party data protections otherwise afforded by the Court are "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[736] To the extent that the facial images, video footage, or other biometric data is obtained from third parties, a function for which the FBI's Next Generation Identification system is actually designed, and paired with biographic information, under the Court's current jurisprudence, such information would not constitute a search or be subject to Fourth Amendment protections.

3. Resource Limitations and Frequency of Occurrence

In *United States v. Garcia*, Judge Posner suggested that certain forms of technological progress may pose a threat to privacy by enabling surveillance to an extent that in earlier times would have been prohibitively expensive.[737] Assuming, arguendo, that remote biometric identification is not a full search within the meaning of the Fourth Amendment (i.e., that it is something less than a full search), one question might be

734. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).

735. *See Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS)*, *supra* note 18.

736. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

737. United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).

whether it falls within an area similar to that carved out under *Terry v. Ohio*.[738] Here, Judge Posner's warning about lifting resource restrictions proves particularly prescient.

In *Terry*, the Court held that the police could stop and frisk a passerby based on reasonable suspicion.[739] The idea was that, in justifying the search, the police officer must be able to point to specific and articulable facts, which, taken together with reasonable inferences from those facts, warrant the intrusion.[740] Those facts have to be judged against an objective standard: whether the information available at that time would justify a person in taking such action.[741] *Terry* dealt with a physical pat down on the outside of the clothes.[742] In 2004, the Court addressed whether merely asking someone their name, in the course of a *Terry* stop, raised a Fourth Amendment issue.[743] In a 5-4 decision, the Court held Nevada's "stop and identify" statute constitutional.[744]

The reasonableness of a search entails balancing the individual's interest in privacy against the government's interest in the specific intrusion.[745] The Supreme Court recognized in *Terry* that the Fourth Amendment requires that courts assume the responsibility of guarding against police conduct that is overbearing or harassing.[746] Noted Fourth Amendment scholar Wayne LaFave reads this as suggesting that "harassment-by-surveillance, at least when there is 'harassment bordering on arrest,' therefore should be viewed as a violation of the Fourth Amendment."[747]

Do biometric identification devices accomplish by technology what constant stops would do if executed by officers of the law? It seems to me that the answer to this is yes. Just as frequent stops of pedestrians and the manual recording of that information would create a record of movement in public space,

738. Terry v. Ohio, 392 U.S. 1, 16 (1968).

739. *Id.* at 30.

740. *Id.* at 21.

741. *Id.*

742. *Id.* at 7.

743. Hiibel v. Sixth Judicial Dist. Court, 542 U.S. 177, 184–85 (2004).

744. *Id.* at 178 ("The Court is now of the view that *Terry* principles permit a State to require a suspect to disclose his name in the course of a *Terry* stop.").

745. *See, e.g.*, United States v. Martinez-Fuerte, 428 U.S. 543, 555 (1976); United States v. Klein, 522 F.2d 296, 300–01 (1st Cir. 1975).

746. Terry v. Ohio, 392 U.S. 1, 16 (1968).

747. LAFAVE, *supra* note 569, § 2.7 at 778–79 (footnotes omitted).

so too might the use of biometric identification devices. In fact, it could create not just frequent records of individuals' movements, but constant records of the same. This appears to be something different than what is contemplated by the Court's jurisprudence in relation to a *Terry* stop. It is a difference that is enabled by the loosening of resource limitations.

It could be argued in response that just because RBI performs a similar function to a *Terry* stop does not mean that it does so in a harassing manner. One could convincingly claim that the level of harassment involved in RBI is actually negligible. In the course of a *Terry* stop, an individual is forced to suspend one's activities. Movement is limited, resulting in a loss of physical and personal freedom. But simply having this information recorded as one passes through space does not (on the surface) appear to entail any physical limitation. Admittedly, this argument assumes that individuals under such surveillance do not alter their movements or behavior because of it. But in such circumstances, the level of harassment may be so small as to be non-existent. Further, even denying the underlying assumption and granting that individuals may change their behavior, surely it would be a convoluted reading of the Court's jurisprudence, to connect this to the physical limitation of a face-to-face encounter.

The problem with this line of argument is that it still assumes a framing based on degree, not kind—i.e., that the level of harassment in RBI is less than the level of harassment in a face-to-face encounter, while the level of monitoring is higher than the level of monitoring in the same. It also rather misses the point, which is the level of information obtained by a relaxation of the resource constraint.

IV. FURTHER POTENTIAL CONSTITUTIONAL CHALLENGES

Privacy concerns are not the only potential constitutional challenge. Fifth Amendment protections against self-incrimination, First Amendment assurance of the right to speech and assembly, and Fifth and Fourteenth Amendment due process concerns similarly present themselves. Yet the associated jurisprudence in each of these areas proves inadequate to address the phenomenon of remote biometric identification.

A. FIFTH AMENDMENT RIGHT AGAINST SELF-INCRIMINATION

Consider the Fifth Amendment, which provides that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself."[748] This provision is rooted in protections against being forced by the government to engage in certain behavior—not (as with the Fourth Amendment), efforts to limit what the government can do directly to an individual. Thus, at the broadest level, the way remote biometric identification presents seems not to implicate the Fifth Amendment.

A practical example will suffice. A government-owned camera using remote biometric identification may be directed at public space in a neighborhood. It seems odd to think of the individual entering that space as being compelled by the government to do so. Similarly, a closed circuit television in a grocery store such as Safeway—owned by a private company—hardly amounts to government compulsion to enter the store. In both instances, the decision to enter the space under surveillance, whence facial recognition or iris scans could be used to ascertain identity, appears to be voluntary. To the extent that either of these decisions is not voluntary (e.g., the need to leave one's home and travel through the neighborhood to get to work, or the need to enter the grocery store in order to buy milk for one's infant), it is not government action that compels it, but rather sheer day-to-day living necessity. It is not just the entering of one or two areas under surveillance, moreover, that an individual encounters in the course of daily life. British studies have noted, for instance, that the average Londoner is caught on camera, in public space, some 300 times per day.[749]

The result of entering into public space, then, where remote biometric technologies can then identify and track one's movements, results in a sort of *caveat civis*—citizens beware. If one is travelling in public, there is a sort of de facto notice that the information could be captured, recorded, and shared. Most of the time, it is not the government demanding that individuals enter public space. Necessity or personal desire—such as wanting to see friends, pursue an education, or find new clothes—may be the driving force. It is thus perhaps unsurprising that no cases have yet to consider FRT, much less FRT

748. U.S. CONST. amend. V.

749. *See* Kevin Werbach, *Sensors and Sensibilities*, 28 CARDOZO L. REV. 2321, 2324 (2007).

paired with video surveillance, in the context of the Fifth Amendment.

But what about the mere provision of the information itself? Could a case be made that the point at which FRT and video technologies narrowly, or RBI more broadly, become communicative or testimonial, such information falls within Fifth Amendment protections? That is, the government may not be forcing you to enter public space, but it is forcing you, once you are in public space, to reveal personal information—such as who you are dating, whether you are pregnant, or whether you were routinely go to topless bars. To the extent that such information becomes testimonial, or communicative, could it fall within the protections of the Fifth Amendment?

In 1966, the Supreme Court addressed questions raised by biometric identification.[750] *Schmerber v. California* dealt with the collection of a blood sample taken involuntarily from a hospitalized patient who had been arrested for driving under the influence.[751] The Warren Court unanimously found that the Fifth Amendment protection against self-incrimination only applies to evidence of a testimonial or communicative nature.[752] Justice Brennan admitted that requiring the petitioner to submit to the withdrawal and chemical analysis of blood amounted to government compulsion.[753] But while the Fifth Amendment might reach one's testimony or communications, it stopped short of protecting against compelling individuals "to submit to fingerprinting, photographing, or measurements, to write or speak for identification, to appear in court, to stand, to assume a stance, to walk, or to make a particular gesture."[754] Compelling biometric data that "makes a suspect or accused the *source* of 'real or physical evidence'" thus fell short of Fifth Amendment protections.[755] The Court noted that the distinction be-

750. Schmerber v. California, 384 U.S. 757, 759 (1966).

751. *Id.*

752. *Id.* at 761 ("We hold that the privilege protects an accused only from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature, and that the withdrawal of blood and use of the analysis in question in this case did not involve compulsion to these ends." (footnote omitted)).

753. *Id.*

754. *Id.* at 764 (footnote omitted).

755. *Id.* (emphasis added). This holding was consistent with the Court's earlier ruling in *Holt v. United States*, in which the question turned on whether requiring a defendant to put on a blouse—to prove that it was owned by the defendant—amounted to compelled testimonial evidence. 218 U.S. 245, 252–53 (1910).

tween physical information and testimonial or communicative interactions may not always be so clear.[756] The key was whether the information provided substituted for evidence for use in criminal proceedings, or whether it could give rise to information that could later be used as evidence.[757]

Successive cases adopted a similar approach. The year after *Schmerber*, in *Gilbert v. California*, the Court extended its reasoning to include handwriting samples, holding that "[a] mere handwriting exemplar, in contrast to the content of what is written, like the voice or body itself, is an identifying physical characteristic outside [the Fifth Amendment's] protection."[758] That same year, the Court addressed identification procedures in the context of a lineup. Several weeks after he had been indicted for bank robbery, the respondent in *United States v. Wade* had been placed in a lineup and required to repeat words similar to those allegedly spoken by the robber, at which point two employees made a positive identification.[759] The Court held that "[n]either the lineup itself nor anything shown by this record that Wade was required to do in the lineup violated his privilege against self-incrimination."[760] The Court explained,

> We have no doubt that compelling the accused merely to exhibit his person for observation by a prosecution witness prior to trial involves no compulsion of the accused to give evidence having testimonial significance. It is compulsion of the accused to exhibit his physical characteristics, not compulsion to disclose any knowledge he might have. It is no different from compelling Schmerber to provide a blood sample or Holt to wear the blouse, and, as in those instances, is not within the cover of the privilege.[761]

The use of his visage or his voice merely as an identifying physical characteristic did not speak to his guilt. In 1973, the Court took a similar line in considering whether the compelled production of voice exemplars violated the Fifth Amendment privilege against compulsory self-incrimination.[762] In 1988, the Court further consolidated its jurisprudence in *Doe v. United States*, a case in which the target of a federal grand jury investigation pled the Fifth Amendment to avoid turning over fur-

756. *Schmerber*, 384 U.S. at 764.
757. *See* Kastigar v. United States, 406 U.S. 441, 444–45 (1972).
758. Gilbert v. California, 388 U.S. 263, 266–67 (1967).
759. United States v. Wade, 388 U.S. 218, 222 (1967).
760. *Id.* at 221.
761. *Id.* at 222.
762. United States v. Dionisio, 410 U.S. 1, 5–6 (1973).

ther information about the existence or location of bank records.[763] In order for evidence to be testimonial, "an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a 'witness' against himself."[764] Certain acts (such as being compelled to furnish a blood sample, provide a handwriting or voice exemplar, stand in a lineup, or wear particular clothing) may thus be incriminating, but still fall outside the privilege.

These cases all addressed the question of immediate identification: individuals asked, on a specific occasion, to provide information that served to identify themselves. To this extent, they replicated the conditions laid out, above, in relation to immediate biometric identification, or IBI: i.e., situations focused on (1) a single person; (2) in close proximity; (3) in relation to custodial detention; (4) in a manner involving notice; and (5) as a one-time occurrence. In these circumstances, the target individuals were being compelled to take steps to provide the data being sought.

RBI, in contrast, identifies (1) multiple individuals; (2) at a distance; (3) moving through public space; (4) absent notice and consent; and (5) in a continuous and on-going manner. Such targets provide evidentiary data simply by moving through public space. The problem is that Fifth Amendment jurisprudence, to the extent that it contemplates the provision of evidence from biometric technologies, does so in the context of IBI—not remote biometric identification.

B. FIRST AMENDMENT FREEDOM OF SPEECH AND ASSOCIATION

What about the second constitutional consideration—First Amendment protections?[765] It is at least theoretically possible for RBI to be subject to challenge on First Amendment grounds, particularly where harm to political or religious speech or association can be demonstrated, or a connection between the target of RBI and the compelling government interest can be severed. Yet, here as well, the doctrine proves inadequate as a meaningful framework.

763. Doe v. United States, 487 U.S. 201, 202 (1988).

764. *Id.* at 210 (footnote omitted).

765. "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." U.S. CONST. amend. I.

Under the Court's First Amendment jurisprudence, the government is prevented from regulating speech directly because of its message.[766] It can, however, regulate actions for reasons not having to do with any expressive message it might entail.[767] The key question is whether such law (a) is within the constitutional power of the government, (b) whether it furthers an important or substantial government interest, (c) whether this interest is unrelated to the suppression of free expression, and (d) whether the incidental restriction on First Amendment freedoms is "no greater than is essential to the furtherance" of the targeted interest.[768] The Court considers expressive public conduct or speech-related public association as falling within the protections of the First Amendment, thus requiring the government to justify its actions on a meaningful law enforcement ground.[769]

In the context of the McCarthy era and rapidly expanding oath and affirmation requirements, the Court found in a number of cases that constitutional violations could arise from the chilling effect of governmental regulations.[770] The Court explained that in such circumstances, a heavy burden lies on the government to demonstrate that the inquiry is necessary to protect a legitimate state interest.[771] Early cases in this area focused on instances in which the target had incurred a direct penalty.[772] They left open the problem of the more generalized harm caused by the individual knowing that they were being subject to surveillance—or the "concomitant fear that, armed with the fruits of those activities, the agency might in the future take some *other* and additional action detrimental to that individual."[773]

In 1972, the Court addressed this question in a challenge to the Department of the Army's surveillance of domestic civilian activity.[774] In a program strikingly close to the capacity rep-

766. *See* Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989).

767. *See id.*

768. United States v. O'Brien, 391 U.S. 367, 377 (1968).

769. Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 257–58 (2002).

770. *See, e.g.*, Baird v. State Bar of Ariz., 401 U.S. 1, 6–7 (1971); Keyishian v. Bd. of Regents of the Univ. of the State of N.Y., 385 U.S. 589, 592 (1967); Lamont v. Postmaster Gen. of the U.S., 381 U.S. 301, 305 (1965).

771. *Baird*, 401 U.S. at 6–7.

772. Laird v. Tatum, 408 U.S. 1, 11 (1972).

773. *Id.*

774. *Id.* at 2.

resented by RBI, the Army had initiated a data-gathering system in which it began monitoring public space.[775] Information was derived from the news media, publications, intelligence agents in attendance at public meetings, and civilian law enforcement agencies.[776] In light of growing civil rights agitation, the military cited in support of the programs its statutory authority to make use of the armed forces to quell insurrection and to respond to domestic violence.[777] The Court ruled in favor of the government: the burden lay on the target to establish the immediate danger of direct injury.[778] The risk, for the Court, would be to limit broad scale investigations while arming civilians with judicial weapons to allow them to penetrate into classified government programs.[779] It was not for the judiciary to second guess the political branches.[780]

Applied to RBI, a strong argument could be marshaled that under *Tatum*, any claim as to a generalized chilling of speech or association would be insufficient to overcome First Amendment obstacles: the government need only demonstrate a sufficient government interest to overcome any objection. Law enforcement, now so tightly interwoven with pressing national security concerns, would appear to meet this test. Indeed, cases following *Tatum* underscored that efforts to claim that the threat of surveillance undermined political speech would henceforward be foreclosed.[781] Whether fear constituted a cognizable harm was irrelevant.[782] *Tatum* here was "clear and categorical": allegations of a subjective chilling effect were simply inadequate.[783]

The Supreme Court has not yet addressed whether the chilling effect claimed with regard to speech extends to photo-

775. *Id.* at 6.

776. *Id.*

777. 10 U.S.C. § 331 (2006) ("Whenever there is an insurrection in any State against its government, the President may, upon the request of its legislature or of its governor if the legislature cannot be convened, call into Federal service such of the militia of the other States, in the number requested by that State, and use such of the armed forces, as he considers necessary to suppress the insurrection.").

778. *Tatum*, 408 U.S. at 15–16.

779. *Id.* at 14–15.

780. *Id.* at 15.

781. United Presbyterian Church v. Reagan, 738 F.2d 1375, 1377–79 (D.C. Cir. 1984).

782. *Id.*

783. *Id.* (citing *Tatum*, 408 U.S. at 13–14).

graphs or video recording of individuals at demonstrations or public meetings. Two lower court decisions, however, have.

In 1975, the Third Circuit considered police surveillance of public meetings, in *Philadelphia Yearly Meeting of Religious Society of Friends v. Tate*.[784] The Philadelphia Police Department, through its Political Disobedience Unit, had compiled about 18,000 files on individuals and groups, as distinct from the department's interrogation and investigation records.[785] The files included information about the targets' political views, associations, personal life, and habits.[786] Some targets were unaware that such files had been compiled.[787] In June 1970, the police went on television, discussed system, and publicly named some of the targets.[788] Four individuals and two organizations thus named brought suit alleging (1) that the practices lacked a nexus to legitimate police purposes and deprived plaintiffs of their right to anonymity in the conduct of their political activity and associations; (2) that the intelligence gathering chilled and deterred plaintiffs in their free exercise of speech and assembly; and (3) that the practices unconstitutionally interfered with the plaintiffs' ability to form lawful political associations focused on unpopular views.[789]

The District Court dismissed the complaint on the grounds of *Tatum*: the mere fact of an investigation was insufficient to find a chilling effect on speech.[790] The Court of Appeals reversed the lower court in part and affirmed in part.[791] Chief Judge Collins Seitz, writing for the court, determined that the complaints of police surveillance and the sharing of information between law enforcement agencies fell short of demonstrating a violation of constitutional rights; however, the allegations regarding sharing information with non-law enforcement parties and disclosing the parties' names on national television provided sufficient basis to state a cause of action.[792] "[M]ere police photographing and data gathering at public meetings" was legally unobjectionable, creating

784. Phila. Yearly Meeting of Religious Soc'y of Friends v. Tate, 519 F.2d 1335, 1337–38 (3d Cir. 1975).
785. *Id.* at 1336.
786. *Id.* at 1336–37.
787. *Id.* at 1337.
788. *Id.*
789. *Id.*
790. *Id.*
791. *Id.* at 1339 (footnote omitted).
792. *Id.*

> at best a so-called subjective chill which the Supreme Court has said is not a substitute for a claim of specific present harm or a threat of specific future harm. Nor does the sharing of this information with other agencies of government having a legitimate law enforcement function give rise to a constitutional violation.[793]

In contrast, dispensing the information to non-law enforcement agencies, as well as to the public, created an entirely different purpose.[794] "It cannot be doubted that disclosure on nationwide television that certain named persons or organizations are subjects of police intelligence files has a potential for a substantial adverse impact on such persons and organizations even though tangible evidence of the impact may be difficult, if not impossible, to obtain."[795]

It could be argued that the distinction drawn in *Philadelphia Yearly*, between information collection and information sharing, rests on tenuous grounds. At a minimum, it seems odd to have a rule governing the legality of a search in which actions that take place long after the initial search end up determining its legality. *Philadelphia Yearly*, moreover, could be said to overread *Tatum*. Whereas the former case suggested that the mere presence of cameras, alone, were insufficient to establish a chilling effect, it could be contended that *Tatum* left open the possibility that the target of such surveillance could demonstrate (a) that the surveillance had occurred and (b) that the individual, in turn, curbed their activities—thus establishing both an objective and subjective chilling of speech. Either way, however, the compelling government interest in ensuring national security would play a role.

The Fourth Circuit has also considered the chilling effect of taking photographs of individuals at public meetings and demonstrations in the context of the First Amendment.[796] The police in Richmond, Virginia at the time maintained a uniformed presence at such gatherings, took photos, and made such records available to other law enforcement agencies.[797] In *Donohoe v. Duling*, the 2-1 panel found the case controlled by *Tatum*.[798] Judge Harrison Winter, however, dissented from the majority, finding that the plaintiffs had both standing to sue and had demonstrated a cause of action entitling them to re-

793. *Id.* at 1337–38.
794. *Id.* at 1338–39.
795. *Id.* at 1339.
796. Donohoe v. Duling, 465 F.2d 196, 197–98 (4th Cir. 1972).
797. *Id.*
798. *Id.* at 201.

lief.[799] For him, *Tatum* was decided by a majority of the Court "on the premise that none of the plaintiffs alleged or tendered any proof to show any harm to himself or any violation of his constitutional rights."[800] In contrast, in the immediate case, three witnesses had been photographed by law enforcement officers, "without their permission and inferably against their will, while they were engaged in the peaceful exercise of their first amendment right to assemble and . . . to petition their government for a redress of their grievances."[801] Other protesters had refused to take part in the meetings once they had been photographed.[802] Whereas *Tatum* considered the fear of the consequences of surveillance, this case contemplated actual harm and an actual violation of rights.[803] The question thus became not whether a chilling effect had occurred, but the *degree* of such chill in light of the surrounding circumstances.[804] This pushed the court to the *O'Brien* test.[805]

Applying this case to RBI, it appears that the question of the harm suffered could change depending upon the location and targets of the surveillance in question. As a threshold matter, whether there is a First Amendment question at all rests to some extent on whether an action has an expressive element—certainly a context-specific inquiry. Much of the activity in which individuals engage while in public may simply not fall into this category. In *Donohoe*, the Fourth Circuit considered more narrowly the collection of photographs at political and religious gatherings. If the FBI were to focus RBI on public space outside of mosques or churches, where preachers might otherwise address crowds, perhaps a stronger case of deterrence, as recognized by Judge Winter, could be made. But, again, to the extent that the government demonstrates a compelling governmental interest, such objections could be overcome. There would still need to be a substantial relationship between the target of the surveillance and the overriding government interest—this suggests a specificity which, depending on the context, may be lacking with regard to RBI. However, the broad range of threats now considered within the national security

799. *Id.* at 202 (Winter, J., dissenting).
800. *Id.* at 204.
801. *Id.*
802. *Id.*
803. *Id.* at 204–05.
804. *Id.* at 205.
805. *Id.* (citing United States v. O'Brien, 391 U.S. 367, 377 (1968)).

domain, and the innumerable sources of such threats, suggests that such a category may be rather broadly devised.[806]

Another point to draw out in this context is whether there may be a less intrusive means to conduct such surveillance. Minimization techniques here deserve notice.[807] Surely it is not necessary for the government to collect all information about all individuals in public space in an effort to prevent crime. This stance assumes that the realistic aim of the law is and ought to be the elimination of all crime, for which complete and perfect information may be necessary.

In *Donohue*, Judge Winter drew attention to this prong of the *O'Brien* test.[808] He noted that gathering information about an entire crowd went beyond what was necessary for the object at hand.[809] The passage, in its application to RBI, is worth quoting at length:

> If it is assumed that there is a legitimate reason for recording the identity and likeness of those who lead others in the peaceful exercise of their first amendment rights, there is no reason why police must engage in wholesale photographing of a demonstration in order to obtain pictures of its leaders. In most instances the leaders are known, if not by the fact that they have applied for a permit for the demonstration, then by the fact that they are at the front of the crowd or giving a speech. Moreover, their identity is usually readily ascertainable from the local news media. I conclude that there is no justification for intimidating all the participants in a demonstration in order to obtain pictures of its leaders.[810]

Judge Winter rejected as preposterous the idea that the police would be using photographs to identify unknown people in a crowd: "I cannot suppose that every time a picture is taken of

806. *See* Laura K. Donohue, *The Limits of National Security*, 48 AM. CRIM. L. REV. 1573, 1722 (2011).

807. *Cf. Donohue*, 465 F.2d at 206 (Winter, J., dissenting) (suggesting that the police objectives could have been achieved "with less interference to first amendment rights").

808. *Id.* at 205–06 ("In dismissing plaintiffs' complaint, the district court justified the practice of the police on the grounds that it (1) allows the police to identify demonstration leaders; (2) permits the police to identify unknown persons from outside the Richmond area who are participating in the demonstration and who have records of being dangerous; (3) deters violence and vandalism; and (4) serves to protect the demonstrators from counter-demonstrators. I am not persuaded that these objectives are furthered by the present police practice or, if they are, that the same results cannot be obtained with less interference to first amendment rights.").

809. *Id.* at 206.

810. *Id.*

an unknown person it is sent to the FBI in order to determine whether that person is dangerous."[811]

Forty years later, this is precisely the aim of NGI and the type of use for which RBI is envisioned by DoD, DHS, and others.[812] Judge Winter considered and rejected the possibility that photography might be used in this way—efforts to do so "would appear to be a useless tool in controlling the crowd on the day of the demonstration."[813] Central to his claim was the time it would take to develop the photographs and to disseminate them—considerations that appear almost quaint in light of modern technology. The current return time for photograph, iris, and fingerprint identification is a matter of seconds, leaving more than enough time for the police to take steps in the course of a meeting or gathering.[814]

Judge Winter raised the question of whether any constitutional limits applied to the gathering of such data on targets who themselves were not suspected of any wrongdoing.[815] In such cases, he surmised, law enforcement agencies could certainly take and exchange pictures.[816] As for whether such photographs deterred violence and vandalism, Judge Winter pointed out that the presence of the police would perform an equivalent function—and one significantly different than monitoring and recording all activities that take place at a demonstration.[817] For Judge Winter, then, "indiscriminate photographing . . . would have little value in deterring crime or apprehending a criminal."[818] Other, less intrusive means could be sought in order to avoid "injecting fear into persons who are peacefully exercising their first amendment rights."[819]

Both Title III and the minimization requirement embedded in FISA recognize the importance of ensuring the least intru-

811. *Id.*

812. *See generally* BIOMETRICS TASK FORCE., *supra* note 25 (discussing how DoD's data system retrieves information on people in the system).

813. *Donohue*, 465 F.2d at 206 (Winter, J., dissenting).

814. *See generally* Press Release, Dep't of Homeland Sec., New Biometric Technology Improves Security and Facilitates U.S. Entry Process for International Travelers 1 (Mar. 2009), *available at* http://www.dhs.gov/xlibrary/assets/usvisit/usvisit_edu_10-fingerprint_consumer_friendly_content_1400_words.pdf (stating that fingerprint technology allows DHS officials to identify criminals and immigration violators in the time that it takes them to stand in line).

815. *Donohue*, 465 F.2d at 206 (Winter, J., dissenting).

816. *See id.*

817. *Id.*

818. *Id.*

819. *Id.*

sive means possible.[820] What would minimization procedures look like, however, with regard to RBI? Consider FRT and surveillance cameras. Absent a specific target, the generalized use of the technology and collection of data does seem to place a rather heavy burden on the public at large, with a broad impact on numerous individuals who are not at the time to have been suspected of any wrongdoing. One could argue that the use of mounted cameras on poles is in fact not intrusive—they sit, silent, and do not physically interrupt or interfere with efforts to convey a message. But this argument, as well as its counter, quickly descends into a subjective argument.

C. FIFTH AND FOURTEENTH AMENDMENT DUE PROCESS PROTECTIONS

The third potential constitutional grounding (outside of the Fourth Amendment) for considering RBI lies in the realm of Fifth and Fourteenth Amendment due process concerns.[821] The central issue here with regard to RBI is the accuracy of the information obtained and the manner in which it is maintained. Perhaps the most authoritative public source on the accuracy of FRT is a report co-authored by Professors Lucas Introna and Helen Nissenbaum and published by New York University's Center for Catastrophe Preparedness and Response.[822] The researchers found that while FRT may prove effective "with relatively small populations in controlled environments, for the verification of identity claims," the effort to use it in more complex settings, where individuals "do not voluntarily self-identify"—i.e., the "face in the crowd" scenario, means that it "[i]s unlikely to become an operational reality for the foreseeable future."[823] The researchers' findings suggest that the technology supporting IBI is more sophisticated—and more accurate—than that undergirding RBI.

This does not mean that the former is without challenges: where an individual's face is pre-submitted to the system, the quality of the image (as well as the quality of the subsequent

820. 18 U.S.C. § 2518(5); U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT 11(b) (on file with author).

821. U.S. CONST. amend. V; *id.* amend. XIV, § 1.

822. LUCAS D. INTRONA AND HELEN NISSENBAUM, N.Y.U. CTR. FOR CATASTROPHE PREPAREDNESS AND RESPONSE, FACIAL RECOGNITION TECHNOLOGY: A SURVEY OF POLICY AND IMPLEMENTATION ISSUES (2010), *available at* http://eprints.lancs.ac.uk/49012/1/Document.pdf.

823. *Id.* at 3.

image submitted for matching) appear to have a significant impact on overall performance.[824] Various other factors could undermine accuracy, such as the environmental conditions in which the image was taken, the time that had elapsed between the images submitted for comparison, the similarity of the cameras used to capture the images, and the size of the gallery.[825] But it does suggest that accuracy could be a problem for the way that DOJ/FBI, DHS, and DoD envision their use of remote identification technologies.[826] The authors explain:

> In the scenario that we have called "the grand prize," an FRS [facial recognition system] would pick out targeted individuals in a crowd. Such are the hopes for FRS serving purposes of law enforcement, national security, and counterterrorism. Potentially connected to video surveillance systems (CCTV) already monitoring outdoor public spaces like town centers, the systems would alert authorities to the presence of known or suspected terrorists or criminals whose images are already enrolled in a system's gallery, or could also be used for tracking down lost children or other missing persons. This is among the most ambitious application scenarios given the current state of technology. Poor quality probe images due to unpredictable light and shadows in outdoor scenes, unpredictable facial orientation, and "noise" from cluttered backgrounds make it difficult for an FRS in the first place to even pick out faces in the images. Challenges posed by the lack of control inherent in most scenarios of this kind are exacerbated by the likelihood of uncooperative subjects. Additionally CCTV cameras are generally mounted high (for protection of the camera itself), looking down into the viewing space, thus imposing a pose angle from above which has been shown to have a strong negative impact on recognition and operate at a distance for which obtaining adequate (90 pixel) interoccular resolution is difficult.[827]

Difficult, though, does not mean impossible. The authors point out, for instance, that the problems associated with scanning crowds could be overcome by forcing traffic through portals, where more of the "complicating factors" could be controlled.[828]

As a constitutional matter, then, it is possible that the reliability of the technologies involved in RBI could give rise to due process concerns. Numerous drug-testing cases in the 1980s, for instance, overturned employee dismissals on the grounds that the urinalysis on which the dismissals were based only provided ninety-five to ninety-nine percent accuracy.[829] The

824. *Id.*

825. *Id.*

826. The report itself was made possible through a grant from the Department of Homeland Security. *Id.* at 2.

827. *Id.* at 20.

828. *Id.*

829. Kenneth P. Nuger, *Biometric Applications: Legal and Societal Consid-*

numbers for many of the technologies involved in RBI are significantly lower, ranging, in some cases, from thirty to sixty percent[830] In the drug testing cases, a cognizable harm directly followed from the use of (potentially inaccurate) tests. To the extent that RBI becomes the basis for criminal conviction, a similar argument could be made. But one need not even go this far. Where biometric devices, for instance, are used for authentication purposes, the denial of permission for a commercial driver to cross state lines may itself result in a due process violation claim.[831]

It is important here to recognize that such claims may only be relevant for a limited time and, as such, should not be relied on as a basis for framing the problem. Not only do estimates vary widely, depending on the technology involved, the system under consideration, and who is doing the testing, but the technology is rapidly improving.[832] Professors Alessandro Acquisti, Ralph Gross, and Fred Stutzman, for instance, of Carnegie Mellon University, recently conducted a study on the use of off-the-shelf FRT software for matching Facebook profiles to students walking across a U.S. college campus.[833] The researchers found that based solely on information provided on the social network site, they could positively identify thirty percent of the students passing through public space. Further experiment led to associating sensitive information (such as the students' personal interests, Social Security numbers, and other information) simply by combining face recognition, data mining algorithms, and statistical re-identification techniques.[834]

erations, http://www.engr.sjsu.edu/biometrics/publications_consideration.html (last visited Nov. 2, 2012).

830. *See generally* ANIL K. JAIN & AJAY KUMAR, BIOMETRICS OF NEXT GENERATION: AN OVERVIEW 12 (2010), *available at* http://biometrics.cse.msu.edu/Publications/GeneralBiometrics/JainKumarNextGenBiometrics_BookChap10.pdf (showing that in some conditions recognition accuracy falls to forty-seven percent).

831. *Id.*

832. INTRONA & NISSENBAUM, *supra* note 822, at 26.

833. *See* ALESSANDRO ACQUISTI, RALPH GROSS, & FRED STUTZMAN, PRIVACY IN THE AGE OF AUGMENTED REALITY 9 (2012), *available at* http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/acquisti-faces-BLACKHAT-draft.pdf; *see also What Facial Recognition Technology Means for Privacy and Civil Liberties*: *Hearing Before the S. Comm on the Judiciary Subcommittee on Privacy, Technology and the Law* (2012) (statement of Professor Alessandro Acquisti, Heinz College and CyLab, Carnegie Mellon University), *available at* http://www.judiciary.senate.gov/pdf/12-7-18AcquistiTestimony.pdf.

834. ACQUISTI, GROSS & STUTZMAN, *supra* note 833, at 1.

The researchers noted that as of 1997, the best FRT program at DoD scored an error rate of some 0.54; but by 2006, the false reject rate had plummeted by two orders of magnitude. At the same time, the amount of information publicly available that could be used to correlate identification efforts had skyrocketed.[835]

The authors of the New York University study reached a similar conclusion about the evolutionary rate of technology. They explained: "There is no doubt that FRT is developing very rapidly. Face Recognition Vendor Test (FVRT) 2006 indicated that FRT could, under certain conditions, outperform humans."[836] The report went on to contemplate the use of FRT in the "grand prize."[837] In the interim, a ready solution stood at hand: systems making use of multi-modal biometric systems[838]—a solution which, it turns out, is precisely the route being followed by government agencies.

The FBI explained in a press release:

> The NGI System will expand on the FBI Criminal Justice Information Services (CJIS) Division's current Integrated Automated Fingerprint Identification System (IAFIS), which is primarily a fingerprint-based identification system operated and maintained in Clarksburg, West Virginia. The NGI System will provide improvements to current services and new functionality for the criminal justice, national security, and civil communities . . . .[839]

In sum, even as the technology is rapidly gaining ground, multi-modal biometric systems further enhance the accuracy of RBI technologies. This significantly undermines the potential for due process challenges under the Fifth and Fourteenth Amendments.

One further consideration with regard to due process and accuracy stems from the role of state and local government in obtaining biometric information. To the extent that state and local governments increasingly occupy the RBI realm and, indeed, act as the handmaidens of federal agencies, Fourteenth Amendment concerns become increasingly relevant. Statutory authorization for the collection of personally identifiable infor-

835. *Id.*

836. INTRONA & NISSENBAUM, *supra* note 822, at 42.

837. *Id.* at 43.

838. *Id.* at 47.

839. Press Release, Fed. Bureau of Investigation, FBI Announces Contract Award for Next Generation Identification System (Feb. 12, 2008), *available at* http://www.fbi.gov/news/pressrel/press-releases/fbi-announces-contract-award-for-next-generation-identification-system.

mation (discussed in Part II), creates a federal right for government agencies to accumulate significant amounts of data. With such statutory authorities, however, also comes the concomitant duty to protect against mistakes, tampering, or unwarranted disclosure. The Privacy Act thus requires agencies to allow for targets to challenge PII held about them. The statute, however, also creates a massive loophole in this requirement, allowing information collected for either law enforcement or national security purposes (and, assumedly, both), to be exempted from individual challenge.

One is thus driven back upon a potential constitutional duty that requires government agencies to maintain information in an accurate manner, with access to such information only provided to the appropriate authorities. A similar question has come before the courts. In 1977, the Supreme Court considered a challenge to the constitutionality of New York statutes requiring the state to be given a copy of each drug prescription and creating security measures for the storage of such information by the state. Justice John Paul Stevens, writing for a unanimous court, held the statutes to be a reasonable exercise of New York's broad police powers.[840] He noted that there were no grounds to assume that the security provisions incorporated into the statute would be inadequate or improperly administered.[841] Such a provision clearly showed an interest in the protection of individual privacy.

> We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data—whether intentional or unintentional—or by a system that did not contain comparable security provisions. We simply hold that this record does not establish an invasion of any right or liberty protected by the Fourteenth Amendment.[842]

The responsible treatment of the data included in the biometric repositories, particularly when entered by state and local governments, thus gives rise to a potential Fourteenth Amendment challenge—one which has not been foreclosed by the Court. Failure to adequately protect such databases against improper use may thus run afoul of constitutional constraints.[843] The problem of pursuing this line of jurisprudence

840. Whalen v. Roe, 429 U.S. 589, 598 (1977).

841. *Id.* at 601–02.

842. *Id.* at 605–06.

843. *See* Steven Goldberg, *Enhancing the Senses: How Technological Advances Shape Our View of the Law*, 109 W. VA. L. REV. 1, 13–14 (2006) (arguing that "a governmental biometric database with inadequate safeguards

with regard to RBI stems, again, from the overlapping law enforcement and national security concerns. Citizens' efforts to obtain information about database processes runs into the immediate wall of government privilege. Exceptions in FOIA for national security matters, paired with state secrets doctrine, may make such information nearly impossible to obtain.[844]

V. REMOTE BIOMETRIC IDENTIFICATION COMES OF AGE

The past decade has witnessed a sudden explosion in remote biometric identification. Congress, however, even as it has required the Executive to develop and use these technologies, has not placed meaningful limits on the use of such powers. Gaps in the 1974 Privacy Act and its progeny, as well as the 1990 Computer Act, in conjunction with explicit exemptions in the Privacy Act and the 2002 E-Government Act, remove most biometric systems from the statutes' remit. As a matter of criminal law, Title III of the 1968 Omnibus Crime Control and Safe Streets Act and Title I of the 1986 Electronic Communications Privacy Act say nothing about RBI. In the national security statutory realm, it is unclear whether remote biometric technologies are currently included within the 1978 Foreign Intelligence Surveillance Act's definition of electronic surveillance. The statute's dependence, moreover, on the distinction between U.S. persons and non-U.S. persons presents a direct challenge to the way in which RBI operates. At the same time, principles enshrined in the statute appear inapplicable to the RBI context. Recourse to constitutional challenge provides little by way of respite: Fourth Amendment jurisprudence fails to address the implications of RBI. Fifth Amendment rights against self-incrimination, First Amendment protections on the right to free speech and free assembly, and Fifth and Fourteenth Amendment due process concerns similarly fall short.

Why is it that the legislature and the courts have been so slow to recognize the challenges posed by these new technologies—and how ought we to think about the questions raised by remote biometric identification?

Part of the problem may be an over-reliance on liberal political thought. Indeed, the entire surveillance debate is domi-

could be challenged by an individual in that database on the theory that the government had violated his rights").

844. H.R. 5164, 98th Cong. (1984) (enacted) (exempting the Privacy Act from FOIA restrictions).

nated by an emphasis on personally identifiable information. On one side of the equation, proponents look to grant agencies the power to collect information on individuals; on the other, opponents attempt to create protections against abuse of the same. As Professor Julie Cohen recognizes, regardless of which position one adopts, the underlying framework rests on liberal theory: individual rights act as entitlements held by autonomous individuals within society, who themselves have the capacity for rational thought.[845] The liberal political tradition thus understands privacy within a broader scheme of legal rights and obligations.[846] Cohen argues that within this rights-based world privacy has become a kind of second class citizen, which in turn has generated debate about whether it is a fundamental right, or whether it is merely socially constructed.[847]

Perhaps one solution, then, would be to begin to think about privacy in a constitutive sense, i.e., as a building block of self and social interaction.[848] The central question thus shifts from "What pre-existing political rights are held by individuals?" to "What role does privacy play in human development?" It gives rise to further inquiry, such as "How does privacy influence the social structure of society?" and "How does it affect the relationship between individuals and the state?" These types of questions include, but go beyond what Cohen refers to as "human flourishing."[849] It is a conversation driven by individual experience and social and political construction.

845. JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 16–17 (2012) (discussing also the principal attributes of the legal subject in liberal political thought).

846. *See id.* (discussing the abstract rights possessed by autonomous individuals).

847. *Id.* at 19.

848. Professor Helen Nissenbaum, for instance, who argues (as a descriptive matter) for co-existent, alternative theories of privacy, embraces both liberal, rights-based theory and approaches that emphasize the social context within which information exchange occurs. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 67–104 (2010). In her view, social norms and values may play a central role in our conception of privacy, with consequences for the broader construction of society. *Id.* Professor Daniel Solove, in turn, argues that technology has driven the concept of privacy beyond recognition. He offers an alternative theory in which overlapping concepts of privacy accompany culturally-dependent social norms. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 9 (2008). The value, therefore, of privacy depends not on individual rights but on the importance of the concept to society. *Id.* at 10. *See* COHEN, *supra* note 845, at 20.

849. COHEN, *supra* note 845, at 14–16.

One of Cohen's most important insights, and one shared by other constructive theorists, is that privacy plays a more central role in human experience than liberal political theory acknowledges. Boundary management, which gives breathing space for subjectivity—and critical subjectivity in particular—depends upon privacy not as an individual right, but as a social good. Cohen notes, "A society that wishes to foster critical subjectivity must cabin the informational and spatial logics of surveillance."[850] Other norms, such as mobility, access to knowledge, and discontinuity, may prove equally important in development of the self and society. There is a broader danger in reducing the self to binary code.

At a minimum, much more work on this front, specifically in regard to how we think about privacy as a constitutive principle in regard to information recording, access and management—and particularly as it relates to new identification technologies—needs to occur. This approach rests not on simply adapting the existing frameworks, but on re-conceiving the place of privacy for self and society.

What makes this inquiry so pressing is that the federal government, to date, has been so eager to take advantage of the new technologies that constitute RBI. At one level, this makes a great deal of sense. To the extent that technology makes officials more efficient, utilizes resources more effectively, and helps to accomplish the aims of government agencies, strong support would naturally follow. This is a rationale adopted by all three branches of government, as illustrated by, e.g., legislative directives to the executive branch to move swiftly to explore biometric technologies (Part I, above), initiatives taken by the Executive branch post-9/11 to develop new systems (Part I, above), and judicial decisions that rest upon the assumption that the new technologies merely do what a single police officer could do by tailing and individual—but more efficiently (Part III, above).

The problem with this approach is that the underlying assumption is wrong. This technology is not simply more efficient. It is different in kind—not degree—to what has come before. These are not just incremental changes to the status quo, which ought to be treated in a manner consistent with traditional framings. Cameras in public space capture significantly more than the naked eye outside the curtilage of the home

850. *Id.* at 31.

might learn. They record, with perfect recall, entire contexts, which may, in conjunction with other biometric and biographic data, reveal new insights into citizens' lives and social networks. The kind of surveillance in question, the length of the surveillance, and the radical reduction in resource limitations all differ.

It is time for Congress—and the courts—to recognize this new form of surveillance. Towards these ends, I have proposed five guidelines to distinguish RBI technologies from those more common in immediate biometric identification. Specifically, RBI allows the government to ascertain the identity (1) of multiple people; (2) at a distance; (3) in public space; (4) absent notice and consent; and (5) in a continuous and on-going manner.[851] The stakes could not be higher for subjecting technologies that fall into this category to more rigorous scrutiny. For what we now face are questions about human development, social construction, and the role of government in the lives of citizens—questions that go well beyond individual rights.

851. There are a range of tools that could be contemplated, as a practical matter, to address the challenges of RBI (e.g., notice, the opportunity to correct misinformation, judicial review, public reporting and accountability, feedback about the effectiveness of analysis, training, security clearances for those with access to information, limitations on data entered into different systems, the length of time it is kept, and the conditions under which analysis may be performed, remedies, and intermediary liability). But exactly how to craft such instruments and what approach to take heavily depends upon the theoretical underpinnings of how to think about privacy and the manner in which new technologies are evaluated and implemented.