Written Testimony of Jennifer Lynch
Staff Attorney with the Electronic Frontier Foundation (EFF)

Senate Committee on the Judiciary
Subcommittee on Privacy, Technology, and the Law

What Facial Recognition Technology Means for Privacy and Civil Liberties

July 18, 2012

Mr. Chairman and Members of the Subcommittee:

Thank you very much for the opportunity to testify today on facial recognition. My name is Jennifer Lynch, and I am an attorney with the Electronic Frontier Foundation (EFF) in San Francisco. For the last few years, first at the Samuelson Law, Technology & Public Policy Clinic at Berkeley Law School and then at EFF, I have studied the privacy implications of new technologies, including facial recognition. I have written and presented on federal, state and local law enforcement efforts to expand biometrics databases by adding facial recognition capabilities and on the impact that would have on all Americans and especially on immigrant communities. At EFF I file and litigate Freedom of Information Act requests, including several related to biometrics and facial recognition, and analyze and report on the records I receive. I have been interviewed for and quoted on biometrics and other privacy-threatening technologies in mainstream and technical press including the *New York Times*, *The Economist, Los Angeles Times*, *Wall Street Journal, NPR, Wired, Huffington Post*, *CNet*, *Forbes*, and elsewhere.

Although the collection of biometrics—including face recognition-ready photographs—seems like science fiction; it is already a well-established part of our lives in the United States. The Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) each have the largest biometrics databases in the world,[1] and both agencies are working to add extensive facial recognition capabilities. The FBI has partnered with several states to collect face recognition-ready photographs of all suspects arrested and booked,[2] and, in December 2011, DHS signed a $71 million dollar contract with Accenture to incorporate facial recognition and allow real-time biometrics sharing with the Department of Justice (DOJ) and Department of Defense (DOD). State and local law-enforcement agencies are also adopting and expanding their own biometrics databases to

---

[1] FBI, *Integrated Automated Fingerprint Identification System*, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis (last visited July 16, 2012); Elizabeth Montalbano, "DHS Expands US-VISIT Biometric Capabilities," *Information Week* (Dec. 22, 2011), http://www.informationweek.com/news/government/security/232300942.

[2] *See* Aliya Sternstein, "FBI to Launch Nationwide Facial Recognition Service," *Nextgov.com* (Oct. 7, 2011), *available at* http://www.nextgov.com/nextgov/ng_20111007_6100.php.

incorporate face recognition, and are using handheld mobile devices to allow biometrics collection in "the field."[3]

The scope of government-driven biometrics data collection is well-matched by private-sector collection. Facebook, which uses face recognition by default to scan all photos uploaded to its site, states that its users uploaded more than 300 million photos *every day* in the three months ending on March 31, 2012.[4] And Face.com, which developed Facebook's face recognition tools and was recently acquired by the company, stated in March that it had indexed 31 billion face images.[5] Other companies, from large technology companies like Google and Apple to small smartphone app providers, also provide face recognition products to their customers, and private companies are using biometric identification for everything from preventing unauthorized access to computers and corporate facilities to preventing unauthorized access to the gym.[6]

Face recognition is here to stay, and, though many Americans may not realize it, they are already in a face recognition database. Facebook refuses to say how many face prints it has in its database and whether it creates a face print for photos of non-Facebook users.[7] However, given that Facebook has approximately 170 million active monthly users in the United States alone, at least 54% of the United States population already has a face print.[8]

Face recognition technology, like other biometrics programs that collect, store, share and combine sensitive and unique data poses critical threats to privacy and civil liberties. Biometrics in general are immutable, readily accessible, individuating and can be highly prejudicial. Face recognition, though, takes the risks inherent in other biometrics to a new level because Americans cannot take precautions to prevent the collection of their image.

---

[3] *See* Emily Steel, "How a New Police Tool for Face Recognition Works," *Wall St. J. Digits Blog* (July 13, 2011) http://blogs.wsj.com/digits/2011/07/13/how-a-new-police-tool-for-face-recognition-works/ (describing the Mobile Offender Recognition and Information System (MORIS), which attaches to an iPhone and allows face, fingerprint and iris scanning and identification). As I have written, law enforcement appears to be using these devices with little or no precursor level of suspicion. *See* Jennifer Lynch*, From Fingerprints to DNA: Biometric Data Collection in U.S. Immigrant Communities and Beyond*, Electronic Frontier Foundation & Immigration Policy Council Whitepaper, 3 (May 23, 2012) available at https://www.eff.org/wp/fingerprints-dna-biometric-data-collection-us-immigrant-communities-and-beyond.

[4] Facebook, *Key Facts: Statistics* (last visited July 9, 2012) http://newsroom.fb.com/content/default.aspx?NewsAreaId=22.

[5] See Yaniv Taigman and Lior Wolf, "Leveraging Billions of Faces to Overcome Performance Barriers in Unconstrained Face Recognition," Face.com, http://face.com/research/faceR2011b.html (last visited Mar. 15, 2012).

[6] Demian Bulwa, "Fingerprint check-in tried at 24 Hour Fitness," *S.F. Chron.* (Aug 23, 2010) http://www.sfgate.com/bayarea/article/Fingerprint-check-in-tried-at-24-Hour-Fitness-3255272.php

[7] For example, many Facebook users regularly upload photographs of their non-Facebook using babies and children and identify these images with a name in the description field for the photo. Others create Facebook profiles for their unborn children. *See* Steven Leckart, "The Facebook-Free Baby," *Wall St. J.*, http://online.wsj.com/article/SB10001424052702304451104577392041180138910.html

[8] This is a conservative estimate based on the latest U.S. population figures. It doesn't account for the fact that Facebook, which uses face recognition to scan all photographs uploaded, may be creating a face print for non-Facebook users as well.

Face recognition allows for covert, remote and mass capture and identification of images—and the photos that may end up in a database include not just a person's face but also how she is dressed and possibly whom she is with. This creates threats to free association and free expression not evident in other biometrics.

Americans cannot participate in society without exposing their faces to public view. Similarly, connecting with friends, family and the broader world through social media has quickly become a daily (and some would say necessary) experience for Americans of all ages. Though face recognition implicates important First and Fourth Amendment values, it is unclear whether the Constitution would protect against over-collection. Without legal protections in place, it could be relatively easy for the government or private companies to amass a database of images on all Americans.

This presents opportunities for Congress to develop legislation that would protect Americans from inappropriate and excessive biometrics collection. The Constitution creates a baseline, but Congress can legislate significant additional privacy protections. As I discuss further below, Congress could use statutes like the Wiretap Act[9] and the Video Privacy Protection Act[10] as models for this legislation. Both were passed in direct response to privacy threats posed by new technologies and each includes meaningful limits and protections to guard against over-collection, retention and misuse of data.

My testimony will discuss some of the larger current and proposed facial recognition collection programs and their implications for privacy and civil liberties in a democratic society. It will also review some of the laws that may govern biometrics collection and will outline best practices for developing effective and responsible biometrics programs—and legislation to regulate those programs—in the future.

Government Use of Facial Recognition Technologies

Law Enforcement and government at all levels in the United States regularly collect biometrics; combine them with biographic data such as name, address, immigration status, criminal record, gender and race; store them in databases accessible to many different entities; and share them with other agencies and governments. These collection programs have, in the past, typically included only one biometric identifier (generally a fingerprint or DNA). However, many are rapidly expanding to include facial recognition-ready photographs.

Federal and State Biometrics Databases

The two largest biometrics databases in the world are the FBI's Integrated Automated Fingerprint System (IAFIS) and DHS's Automated Biometric Identification System (IDENT), a part of its U.S. Visitor and Immigration Status Indicator Technology (US-VISIT) program.[11] Each database holds more than 100 million records—more than one

[9] 18 U. S. C. §§2510–2522.

[10] 18 U.S.C. § 2710.

[11] Elizabeth Montalbano, "DHS Expands US-VISIT Biometric Capabilities," *Information Week* (Dec. 22, 2011), http://www.informationweek.com/news/government/security/232300942.

third the population of the United States. Although each of these databases currently relies on fingerprints, both are in the process of incorporating facial recognition.

IAFIS's criminal file includes records on people arrested at the local, state, and federal level and latent prints taken from crime scenes. IAFIS's civil file stores biometric and biographic data collected from members of the military, federal employees and as part of a background check for many types of jobs, such as childcare workers, law-enforcement officers, and lawyers.[12] IAFIS includes over 71 million subjects in the criminal master file and more than 33 million civil fingerprints,[13] and supports over 18,000 law-enforcement agencies at the state, local, tribal, federal, and international level.

IDENT stores biometric and biographical data for individuals who interact with the various agencies under the DHS umbrella, including Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), Customs and Border Protection (CBP), the Transportation Security Administration (TSA), the U.S. Coast Guard, and others.[14] Through US-VISIT, DHS collects fingerprints from all international travelers to the United States who do not hold U.S. passports.[15] USCIS also collects fingerprints from citizenship applicants and all individuals seeking to study, live, or work in the United States.[16] And the State Department transmits fingerprints to IDENT from all visa applicants.[17] IDENT processes more than 300,000 "encounters" every day and has 130 million records on file.[18]

In addition to the federal databases, each of the states has its own biometrics databases, and some larger metropolitan areas like Los Angeles also have regional databases. The

---

[12] *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS)* (hereinafter "2008 IPS PIA"), FBI (June 9, 2008), http://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system.

[13] *See* http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis (last visited Apr. 26, 2012).

[14] *See* DHS, "Privacy Impact Assessment for the Automated Biometric Identification System (IDENT)," (July 31, 2006), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_ident_final.pdf.

[15] Customs and Border Protection (CBP) feeds biometrics data into IDENT while also maintaining its own database, called TECS, which includes personally identifiable information on and biometrics obtained from travelers crossing the border into the United States. *See* DHS, "Privacy Impact Assessment for the TECS System: CBP Primary and Secondary Processing" ("TECS PIA"), DHS/CBP/PIA-009(a), (Dec. 22, 2010), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs-sar-update.pdf.

[16] DHS, "Privacy Impact Assessment for the Refugees, Asylum, and Parole System and the Asylum Pre-Screening System" (Nov. 24, 2009), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_rapsapss.pdf. USCIS also maintains its own database of "biometric images," including a digital photograph and signature, both of which appear on an applicant's naturalization certificates. *See* DHS, "Privacy Impact Assessment Update for the Computer Linked Application Information Management System, DHS/USCIS/PIA-015(a)" (Aug. 31, 2011), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_claimsupdate.pdf (describing capturing of "digitized biometric images" through the Benefits Biometric Support System (BBSS)).

[17] *See* DHS, "Government Agencies Using US-VISIT," http://www.dhs.gov/files/programs/gc_1214422497220.shtm.

[18] Elizabeth Montalbano, "DHS Expands US-VISIT Biometric Capabilities," *Information Week* (Dec. 22, 2011), http://www.informationweek.com/news/government/security/232300942.

prints entered into these databases are shared with the FBI, and under the Secure Communities program, with DHS.

Incorporating Face Recognition Capabilities into Existing Government Databases
In the last few years, federal, state and local governments have been pushing to develop "multimodal" biometric systems that collect and combine two or more biometrics (for example, photographs and fingerprints[19]), arguing that collecting multiple biometrics from each subject will make identification systems more accurate.[20] The FBI's Next Generation Identification (NGI) database represents the most robust effort to introduce and streamline multimodal biometrics collection. FBI has stated it needs "to collect as much biometric data as possible . . . and to make this information accessible to all levels of law enforcement, including International agencies."[21] Accordingly, it has been working "aggressively to build biometric databases that are comprehensive and international in scope."[22]

The biggest and perhaps most controversial change brought about by NGI will be the addition of face-recognition ready photographs.[23] The FBI has already started collecting such photographs through a pilot program with a handful of states.[24] Unlike traditional mug shots, the new NGI photos may be taken from any angle and may include close-ups of scars, marks and tattoos.[25] They may come from public and private sources, including from private security cameras, and may or may not be linked to a specific person's record (for example, NGI may include crowd photos in which many subjects may not be identified). NGI will allow law enforcement, correctional facilities, and criminal justice agencies at the local, state, federal, and international level to submit and access photos, and will allow them to submit photos in bulk.

The FBI has stated that a future goal of NGI is to allow law-enforcement agencies to identify subjects in "public datasets," which could include publicly available

---

[19] Existing biometric databases have allowed users to input some photographs, but they have been limited to traditional mug shots and have not incorporated facial recognition capabilities. *See* 2008 IPS PIA, http://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system.

[20] *Next Generation Identification*, FBI, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi (last visited April 27, 2012).

[21] *See Statement: Interoperability Initiatives Unit* (December 2010), Bates No. SC-FBI-FPL-1043, available at http://uncoverthetruth.org/wp-content/uploads/S-Comm-Hot-Docs-Released-11-10-11.zip (download archive; unzip; open "SC-FBI-FPL-1043.pdf")

[22] *Id.*

[23] Once NGI is complete, it will include iris scans, palm prints, and voice data, in addition to fingerprints.

[24] According to *Nextgov.com*, these states include Michigan, Washington, Florida, and North Carolina. *See* Aliya Sternstein, "FBI to Launch Nationwide Facial Recognition Service," *Nextgov.com* (Oct. 7, 2011), *available at* http://www.nextgov.com/nextgov/ng_20111007_6100.php. However, recently-released records from an FBI Criminal Justice Information Services Advisory Board meeting show that the FBI signed MOUs in December 2011 with Maryland, Michigan and Hawaii and may also be working with Oregon. *See* Jennifer Lynch, "FBI's Facial Recognition is Coming to a State Near You," *EFF.org* (forthcoming) https://www.eff.org/deeplinks/2012/07/fbis_facial_recognition_coming_state_near_you.

[25] *See* 2008 IPS PIA, http://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system.

photographs, such as those posted on Facebook or elsewhere on the Internet.[26] Although a 2008 FBI Privacy Impact Assessment (PIA) stated that the NGI/IAFIS photo database does not collect information from "commercial data aggregators," the PIA acknowledged this information could be collected and added to the database by other NGI users such as state and local law-enforcement agencies.[27] The FBI has also stated that it hopes to be able to use NGI to track people as they move from one location to another.[28]

Another big change in NGI will be the addition of non-criminal photos. If someone applies for any type of job that requires fingerprinting or a background check, his potential employer could require him to submit a photo to the FBI. And, as the 2008 FBI PIA notes, "expanding the photo capability within the NGI [Interstate Photo System] will also expand the searchable photos that are currently maintained in the repository." Although noncriminal information has always been kept separate from criminal, the FBI is currently developing a "master name" system that will link criminal and civil data and will allow a single search query to access all data. The Bureau has stated that it believes that electronic bulk searching of civil records would be "desirable."[29]

DHS is poised to expand IDENT to include face recognition, which would further increase data sharing between DHS and DOJ through Secure Communities and between both agencies and DOD through other programs.[30] DHS has not yet released a Privacy Impact Assessment discussing this change.

Technological Advancements Will Make Face Recognition More Prevalent
Recent advancements in camera and surveillance technology over the last few years support law enforcement goals to use face recognition to track Americans. For example, the National Institute of Justice has developed a 3D binocular and camera that allows realtime facial acquisition and recognition at 1000 meters.[31] The tool wirelessly transmits images to a server, which searches them against a photo database and identifies the photo's subject. As of 2010, these binoculars were already in field-testing with the Los Angeles Sheriff's Department. Presumably, the back-end technology for these binoculars

---

[26] *See, e.g.,* Richard W. Vorder Bruegge, *Facial Recognition and Identification Initiatives*, 5, FBI available at http://biometrics.org/bc2010/presentations/DOJ/vorder_bruegge-Facial-Recognition-and-Identification-Initiatives.pdf (noting a goal of NGI is to "Identify[ ] subjects in public datasets").

[27] *See* 2008 IPS PIA, http://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system.

[28] *See* Vorder Bruegge, *Facial Recognition and Identification Initiatives*, 5.

[29] *See* 2008 IPS PIA, http://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system. The FBI has recognized that "electronic bulk searching of civil file images (such as via facial recognition technology) would constitute a significant new privacy consideration," *id.*, but the FBI has not yet released a new PIA.

[30] *See* "Accenture Awarded Biometric Identity System Contract from U.S. Department of Homeland Security," *Wall Street Journal Market Watch* (Dec. 21, 2011), at http://www.marketwatch.com/story/accenture -awarded-biometric-identity-system-contract-from-us-department-of-homeland-security-2011-12-21; Elizabeth Montalbano, "DHS Expands US-VISIT Biometric Capabilities," *Information Week* (Dec. 22, 2011), http://www.informationweek.com/news/government/security/232300942.

[31] William Ford, *State of Research, Development and Evaluation at NIJ*, 17, National Institute of Justice, http://biometrics.org/bc2010/presentations/DOJ/ford-State-of-Research-Development-and-Evaluation-at-NIJ.pdf.

could be incorporated into other tools like body-mounted video cameras or the MORIS (Mobile Offender Recognition and Information System) iPhone add-on that some police officers are already using.[32]

Private security cameras and the cameras already in use by police departments have also advanced. They are more capable of capturing the details and facial features necessary to support facial recognition-based searches, and the software supporting them allows photo manipulation that can improve the chances of matching a photo to a person already in the database. For example, Gigapixel technology, which creates a panorama photo of many megapixel images stitched together (like those taken by security cameras), allows anyone viewing the photo to drill down to see and tag faces from even the largest crowd photos.[33] It also shows not just a face but also what that person is wearing; what books and political or religious materials he is carrying; and whom he is with. And image enhancement software, already in use by some local law enforcement, can adjust photos "taken in the wild"[34] so they work better with facial recognition searches.

Cameras are also being incorporated into more and more devices that are capable of tracking Americans and that can provide that data to law enforcement. For example, one of the largest manufacturers of highway toll collection systems filed a patent application in 2011 to incorporate cameras into the transponder that sits on the dashboard in your car.[35] This manufacturer's transponders are already in 22 million cars, and law enforcement already uses this data to track subjects. While a patent application does not mean the company is currently manufacturing or trying to sell the devices, it certainly shows it's interested.

Interoperability and Data Sharing

Before September 11, 2001, the federal government had many policies and practices in place to silo data and information within each agency. Since that time the government has enacted several measures that allow—and in many cases require—information sharing within and among federal intelligence and federal, state, and local law-enforcement agencies.[36] For example, currently the FBI, DHS, and Department of Defense's biometrics databases are interoperable, which means the systems can easily share and

---

[32] *See* Emily Steel, "How a New Police Tool for Face Recognition Works," *Wall St. J. Digits Blog* (July 13, 2011) http://blogs.wsj.com/digits/2011/07/13/how-a-new-police-tool-for-face-recognition-works/.

[33] James Fallows, "Technology Is Our Friend ... Except When It Isn't," *The Atlantic* (Aug. 27, 2011) http://www.theatlantic.com/technology/archive/2011/08/technology-is-our-friend-except-when-it-isnt/244233/.

[34] *Pinellas County Sheriff's Office: DHS Future Opportunities*, 10 (2010) http://biometrics.org/bc2010/presentations/DHS/mccallum-DHS-Future-Opportunities.pdf.

[35] Bob Sullivan, "Gov't cameras in your car? E-toll patent hints at Big Brotherish future," *MSN* (Oct. 14, 2011) http://redtape.msnbc.msn.com/_news/2011/10/14/8308841-govt-cameras-in-your-car-e-toll-patent-hints-at-big-brotherish-future.

[36] This was achieved through provisions in the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001), several Executive Orders (Exec. Order No. 13356, 69 C.F.R. 53599 (2004), Exec. Order No. 13355, 69 C.F.R. 53593 (2004), Exec. Order No. 13354, 69 C.F.R. 53589 (2004), Exec. Order No. 13311, 68 C.F.R. 45149 (2003)), and the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004).

exchange data.[37] This has allowed information sharing between FBI and DHS under ICE's Secure Communities program.[38]

And states are collecting and sharing biometric data with the federal government as well. At least 31 states have already started using some form of facial recognition with their DMV photos,[39] generally to stop fraud and identity theft, and the FBI has already worked with North Carolina, one of a handful of states reported to be in the NGI pilot program, to track criminals using the state's DMV records.[40] States also share fingerprints (and face prints soon) indirectly with DHS through Secure Communities. According to the FBI, NGI will allow all states to share and access face prints as easily as they now share and access fingerprints by 2014.[41]

The federal government also exchanges biometric data with foreign governments through direct and ad-hoc access to criminal and terrorist databases.[42] And ICE and the FBI share biometric data on deportees with the countries to which they are deported.[43]

---

[37] The National Institute for Standards and Technology (NIST), along with other standards setting bodies, has developed standards for the exchange of biometric data. See National Institute for Standards and Technology, ANSI/NIST-ITL 1-2011, *American National Standard for Information Systems: Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information* (2011), available at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=910136.

[38] For more on Secure Communities, *see* Michele Waslin, *The Secure Communities Program: Unanswered Questions and Continuing Concerns*, Immigration Policy Center (Nov. 2011). Similarly, DHS is now sharing its data on asylum applicants more broadly with non-DHS agencies, per federal regulation 8 CFR §208.6(a). According to a June 30, 2011, Privacy Impact Assessment, DHS now shares the entire Refugees, Asylum and Parole Services (RAPS) database with the National Counter Terrorism Center (NCTC), a division of the Office of the Director of National Intelligence, under a Memorandum of Understanding (MOU). Dep't of Homeland Sec., *Privacy Impact Assessment Update for the Refugees, Asylum, and Parole System and the Asylum Pre-Screening System,* DHS/USCIS/PIA-027(a) (June 30, 2011), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ raps_update_nctc.pdf. DHS has been sharing asylum data with the FBI since October 8, 2001, per an MOU signed by the agencies on that date. See USCIS Asylum Division, *Fact Sheet on Confidentiality*, 6 (June 15, 2005), available at http://www.usa-federal-forms.com/uscis-index-html/uscis-fact-sheet-on-confidentiality-uscis-5413.html.

[39] Thomas Frank, "Four states adopt 'no-smiles' policy for driver's licenses," *USA Today*, (May 26, 2009) http://www.usatoday.com/news/nation/2009-05-25-licenses_N.htm.

[40] Mike Baker, "FBI uses facial-recognition technology on DMV photos," *USA Today* (Oct. 13, 2009), http://www.usatoday.com/tech/news/2009-10-13-fbi-dmv-facial-recognition_N.htm. British Columbia attempted to use its DMV's face recognition database to identify people involved in the 2011 Stanley Cup riots, though this was later determined by B.C.'s Privacy Commissioner, Elizabeth Denham, to be a violation of Canada's privacy law. Jonathan Fowlie, "Court order required to use facial recognition to identify Stanley Cup rioters," *Vancouver Sun* (Feb. 17, 2012). http://www.vancouversun.com/business/Court+order+required+facial+recognition+identify+Stanley+rioters/6163995/story.html.

[41] *See* Kimberley Del Greco, "FBI Facial Services Program," FBI 5 (Sept. 29, 2011) *available at* http://www.biometrics.org/bc2011/presentations/DOJ/0929_1105_BrA_DelGreco.pdf.

[42] The FBI's Criminal Justice Information Service (CJIS) division has information-sharing relationships with 77 countries, and is working with several countries to allow real-time access to their respective biometrics databases. *See* FBI/CJIS Advisory Policy Board Identification Services Subcommittee, *Issue Paper: Biometrics Information Sharing Update* (Spring 2011), Bates No. SC-FBI-FPL-1088-89, available at http://uncoverthetruth.org/wp-content/uploads/S-Comm-Hot-Docs-Released-11-10-11.zip (download archive; unzip; open "SC-FBI-FPL-1081.pdf") (noting these relationships are "in the form of both informal

Private Sector Use of Facial Recognition Technologies[44]

Private sector use of facial recognition has expanded exponentially in the last few years as well. Facebook uses face recognition for each of its 900 million users.[45] Google offers face recognition to its 170 million Google+ users,[46] and Google and Apple both provide face recognition capabilities in their photo editing systems.[47] App developers offer face recognition to unlock a phone[48] or make tagging easier,[49] and software and hardware developers and manufacturers offer face recognition systems to identify users, and prevent unauthorized access to documents, computers and facilities.

Due to the large number of Facebook users and the fact that these users actively tag each other and themselves in photos, Facebook's face recognition system is the most robust and well-developed of all of these private sector products, and will likely become even more so with the recent purchase of Face.com. Facebook allows users to tag themselves in photos they upload and be tagged in others' photos. Facebook's "Tag Suggest" feature, introduced in December 2010, uses face recognition to automatically match uploaded photos to other photos a Facebook user is tagged in, grouping similar photos together and

---

(ad hoc, verbal) agreements and formal agreements (Memoranda of Agreement, Memoranda of Understanding, Letter of Cooperation).").

[43] *Id.* at SC-FBI-FPL-1089; DHS, "Privacy Impact Assessment for the Automated Biometric Identification System (IDENT)," 8 (July 31, 2006) available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_ident_final.pdf. This kind of biometrics sharing could prove disastrous for repatriated refugees or immigrants from countries with a history of ethnic cleansing.

[44] My testimony focuses on face recognition, rather than face detection. However, for an excellent discussion of face detection and digital signage, *see* Pam Dixon, "The One-Way-Mirror Society: Privacy Implications of the new Digital Signage Networks," *World Privacy Forum* (Jan 27, 2010) *available at*: www.ftc.gov/os/comments/privacyroundtable/544506-00112.pdf; *see also* Harley Geiger, "Seeing is ID'ing: Facial Recognition & Privacy," Center for Democracy & Technology (Decl 6, 2011) https://www.cdt.org/report/seeing-iding-facial-recognition-and-privacy.

[45] Facebook, "Newsroom: Key Facts: Statistics," http://newsroom.fb.com/content/default.aspx?NewsAreaId=22 (last visited July 10, 2012).

[46] The Google+ "Find My Face" feature is different from Facebook's facial recognition tools because, unlike Facebook, users must first opt-in to the system. Chester Wisniewski, "Facial recognition comes to Google+, but unlike Facebook it's opt-in," *Naked Security* (Dec. 9 2011) http://nakedsecurity.sophos.com/2011/12/09/google-introduces-facial-recognition-feature-opt-in-unlike-facebooks-effort/; Matt Steiner, "Making photo tagging easier with Find My Face," *Google*, https://plus.google.com/110260043240685719403/posts/jKQ35ajJ4EU.

[47] *See* Matt Hickey, "Picasa Refresh Brings Facial Recognition," *TechCrunch* (Sept. 2, 2008) http://techcrunch.com/2008/09/02/picasa-refresh-brings-facial-recognition/; Wilson Rothman, "What To Know About iPhoto '09 Face Detection and Recognition," *Gizmodo* (Jan. 29, 2009) http://gizmodo.com/5141741/what-to-know-about-iphoto-09-face-detection-and-recognition.

[48] Christina Bonnington, "FaceVault App Brings Facial Recognition Unlocking to iOS," *Wired Gadget Lab Blog* (April 25, 2012) http://www.wired.com/gadgetlab/2012/04/facevault-app-face-recognition/.

[49] Face.com developed an app called KLIK that allowed users to tag people in photographs before the photo was even taken. However, after Facebook bought Face.com, the app was removed from the Apple app store. *See* David Murphy, "Facebook Kills Face.com Face-Recognition APIs, KLIK app," *PC Magazine* (July 7, 2012) http://www.pcmag.com/article2/0,2817,2406822,00.asp.

suggesting the name of a user's friend in the photo.[50] Facebook markets this tool by stating it will make sorting, tagging and finding photos easier,[51] but it does not make clear that the feature will create a unique biometric—a faceprint—for all its users.

Facebook has stirred up significant controversy with its face recognition tools, in large part because it turned these features on by default. It first enrolled all its users in the system without prior consent and then continued to opt-in users every time they uploaded a photograph. Users may opt-out of tagging on a photo-by-photo basis, but opting out of the system as a whole is complicated. Given the steps necessary to delete the face print "summary" data associated with each user's account[52] and the fact that Facebook uses persuasive language to try to dissuade users from deleting the data completely,[53] it is unlikely most users would go this far. And even if a user deletes the summary data, it is unclear whether taking this step will prevent Facebook from continuing to collect biometric data going forward.[54] As a result of these policies, Facebook has amassed possibly the largest database of face prints in the world[55]—with face prints for about 1/7 of the world population[56]—and will continue to collect more and more face prints every day as more users join the site.

Facebook and other companies using facial recognition combine this data with sensitive and personal biographic data and information on users' networks and associations, exacerbating privacy concerns. Facebook requires each of its users to sign up under their

---

[50] Justin Mitchell, "Making Photo Tagging Easier," *The Facebook Blog* (Dec. 15, 2010), https://www.facebook.com/blog.php?post=467145887130.

[51] *Id.* (noting, "[n]ow if you upload pictures from your cousin's wedding, we'll group together pictures of the bride and suggest her name. Instead of typing her name 64 times, all you'll need to do is click 'Save' to tag all of your cousin's pictures at once.").

[52] *Id*. (noting users may turn off automatic tagging and remove tags added by others); *See also* Eva Galperin, "How to Disable Facebook's Facial Recognition Feature," *EFF* (June 9, 2011) www.eff.org/deeplinks/2011/06/how-disable-facebooks-facial-recognition-feature; Electronic Privacy Information Center (EPIC), "Complaint: In the Matter of Facebook, Inc, and the Facial Identification of Users," 12-15 (June 10, 2011) *available at* http://epic.org/privacy/facebook/EPIC_FB_FR_FTC_ Complaint_ 06_10_11.pdf.

[53] Facebook, "How Can I Turn Off Tag Suggestions?" https://www.facebook.com/help/?faq= 187272841323203#How-can-I-turn-off-tag-suggestions ("Before you opt out of using this feature, we encourage you to consider how tag suggestions benefit you and your friends. Our tagging tools . . . are meant to make it easier for you to share your memories and experiences with your friends.")

[54] *Id.* EPIC Complaint at 16.

[55] Facebook users uploaded more than 300 million photos *every day* in the three months ending on March 31, 2012. Facebook, *Key Facts: Statistics* (last visited July 9, 2012) http://newsroom.fb.com/content/ default.aspx?NewsAreaId=22. *See also* Facebook Photo Trends [INFOGRAPHIC], *PIXABLE* (Feb. 14, 2011) http://blog.pixable.com/2011/02/14/facebook-photo-trends-infographic/ (estimating that as of Summer 2011, users would have uploaded 100 billion photos to Facebook). Face.com, which developed face recognition tools for Facebook and was recently acquired the company, stated in March that it had indexed 31 billion face images. *See* Yaniv Taigman and Lior Wolf, "Leveraging Billions of Faces to Overcome Performance Barriers in Unconstrained Face Recognition," *Face.com*, http://face.com/research/faceR2011b.html (last visited Mar. 15, 2012).

[56] Facebook estimates it has 900 million users. Facebook, "Newsroom: Key Facts: Statistics," http://newsroom.fb.com/content/default.aspx? NewsAreaId=22 (last visited July 10, 2012). The world population is currently estimated at between six and seven billion people.

real names,[57] and then makes users' names, profile photos, gender and networks public by default.[58] Facebook is designed to promote social engagement, and as part of this users can and do provide extensive additional personal information, from email addresses and birthdates to partners' and family members' names, dating preferences, activities and interests, location information, and political and religious beliefs. Facebook also encourages users to communicate with each other through status updates, "likes," posts on other users' walls, and direct messages. Facebook then records all of this information as part of the user's profile, along with other less evident information, such as when users look at another person's profile; when they search for their friends; location, time and date information recorded in their photos; GPS information; and which device or computer they use to log into their account.[59] Through all of this, Facebook establishes associations between and among users and between users and the companies, organizations and causes they find relevant to their lives. All of this information is stored indefinitely by Facebook and, depending on a user's privacy settings, may be available beyond a user's friends or networks—even available to the public at large.

Some or all of this information may be shared with third parties such as other companies, app developers, and advertisers, depending on a user's privacy settings. In addition, the government regularly reviews and requests this data to verify citizenship applications,[60] for evidence in criminal cases,[61] and to look for threats to U.S. safety and security.[62]

---

[57] *See* Emil Protalinski, "Facebook has over 845 million users," *ZDNet* (Feb. 1, 2012), http://www.zdnet.com/blog/facebook/facebook-has-over-845-million-users/8332; Facebook "Statement of Rights and Responsibilities" (April 26, 2011), https://www.facebook.com/legal/terms ("Facebook users provide their real names and information . . . You will not provide any false personal information on Facebook[.]").

[58] Facebook, "Understand Your Internet Search Listing: Is my information visible to people who aren't logged into Facebook?" https://www.facebook.com/help/privacy/public-search-listings (last visited July 10, 2012).

[59] Facebook, "Information we receive and how it is used: Other information we receive about you," https://www.facebook.com/about/privacy/your-info#inforeceived (last visited July 10, 2012).

[60] *See* Jennifer Lynch, "Applying for Citizenship? U.S. Citizenship and Immigration Wants to Be Your 'Friend,'"*EFF* (Oct. 12, 2010), https://www.eff.org/deeplinks/2010/10/applying-citizenship-u-s-citizenship-and (describing how USCIS agents "friend" applicants for citizenship on social networking sites in order to monitor them).

[61] In warrant for Facebook data, the Department of Justice Criminal Division regularly requests all photos in which a user is tagged. *See* Jennifer Lynch, "DOJ Wants to Know Who's Rejecting Your Friend Requests," *EFF* (Jan. 24, 2012), https://www.eff.org/deeplinks/2012/01/doj-wants-know-who%E2%80%99s-rejecting-your-friend-requests.

[62] Jennifer Lynch, "New FOIA Documents Reveal DHS Social Media Monitoring During Obama Inauguration," *EFF* (Oct. 13, 2010), https://www.eff.org/deeplinks/2010/10/new-foia-documents-reveal-dhs-social-media; Jennifer Lynch, "Government Uses Social Networking Sites for More than Investigations," EFF.org (Aug. 16, 2010), https://www.eff.org/deeplinks/2010/08/government-monitors-much-more-social-networks. The FBI is currently looking for software to make its mining of social-media data more efficient and to allow it to map communities of interest. *See* Jim Giles, "FBI releases plans to monitor social networks," *New Scientist* (Jan. 25, 2012), http://www.newscientist.com/blogs/onepercent/2012/01/fbi-releases-plans-to-monitor.html.

As discussed in further detail below, few laws regulate private biometric collection on this scale. In general the public must rely on a company's privacy policies, terms of use, and user-managed privacy settings. However, as the public has seen with the extensive changes Facebook has made to its privacy settings and policies,[63] the fact that it implemented an opt-out based facial recognition system with little fanfare or explanation, and that the first facial recognition app developed to make tagging even easier (KLIK) was quickly hacked to allow access to private information in users' Facebook and Twitter accounts and automatically "recognize" anyone walking down the street,[64] industry self-regulation and consumer control are not enough to protect against critical privacy and security risks inherent in facial recognition data collection.

Concerns about Biometrics, Databases, and Data Sharing

The extensive collection and sharing of biometric data at the local, national, and international level should raise significant concerns among Americans. Data accumulation and sharing can be good for solving crimes across jurisdictions or borders, but can also perpetuate racial and ethnic profiling, social stigma, and inaccuracies throughout all systems and can allow for government tracking and surveillance on a level not before possible.

Some of these concerns are endemic to all data collection and are merely exacerbated by combining biographic data with any non-changeable biometric. For example, courts have recognized the "social stigma" involved with merely having a record in a criminal database.[65] Additionally, data inaccuracies—such those common in immigration[66] and

---

[63] *See* Matt McKeon, Infographic: "The Evolution of Privacy on Facebook," http://mattmckeon.com/facebook-privacy/ (last visited July 11, 2012).

[64] *See* http://ashkansoltani.org/docs/face_palm.html (describing how independent privacy and security researcher Ashkan Soltani hacked Face.com's KLIK app); *See also* Alessandro Acquisti, Face Recognition Study—FAQ, http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/; Will Oremus, "Facebooked in the Crowd," *Slate.com* (June 19, 2012) http://www.slate.com/blogs/future_tense /2012/06/19/facebook_buys_face_com_will_mobile_facial_recognition_kill_privacy_.html (describing Acquisti's research combining "off-the-shelf facial recognition software . . . with Facebook data and a computer algorithm to guess, not only people's names, but in some cases their social security numbers, based solely on snapshots taken with a webcam").

[65] *Menard v. Saxbe*, 498 F.2d 1017, 1024 (D.C. Cir. 1974) ("disabilities flowing from a record of arrest have been well documented: There is an undoubted 'social stigma' involved in an arrest record. It is common knowledge that a man with an arrest record is much more apt to be subject to police scrutiny -- the first to be questioned and the last to be eliminated as a subject in any investigation. . . . Most significant is its use in connection with subsequent inquiries on applications for employment and licenses to engage in certain fields of work. An arrest record often proves to be a substantial barrier to employment." Id. at 1024" (internal citations and footnotes omitted)).

[66] *See generally* Joan Friedland, National Immigration Law Center, *INS Data: The Track Record*, available at www.nilc.org/document.html?id=233 (citing multiple Government Accountability Office and Inspector General reports on inaccuracies in immigration records). These problems persist. *See generally, e.g,* U.S. Government Accountability Office (GAO), *Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain*, GAO-11-146 (Jan. 18, 2011), available at http://www.gao.gov/products/ GAO-11-146 (noting errors in USCIS's e-Verify system and difficulties in correcting those errors). This has happened with the Secure Communities program, where approximately 3,600 United States citizens have been caught up in the program due to incorrect immigration records. *See, e.g.,* Aarti Kohli, et al.

Automated Targeting System[67] records—become much more damaging and difficult to correct as they are perpetuated through cross-database sharing.

Data sharing can also mean that data collected for non-criminal purposes, such as immigration-related records or employment verification, are combined with and used for criminal or national-security purposes with little or no standards, oversight, or transparency. When some of this data comes from sources such as local fusion centers and private security guards in the form of Suspicious Activity Reports (SARs),[68] it can perpetuate racially or politically motivated targeting.[69]

Standardization of biometrics data (necessary to enable data sharing) causes additional concerns. Once data are standardized, they become much easier to use as linking identifiers, not just in interactions with the government but also across disparate databases and throughout society. For example, Social Security numbers were created to serve one purpose—to track wages for Social Security benefits—but are now used to identify a person for credit and background checks, insurance, to obtain food stamps and student loans, and for many other private and government purposes.[70] If biometrics become similarly standardized, they could replace Social Security numbers, and the next time someone applies for insurance, sees her doctor, or fills out an apartment rental application, she could be asked for her face print. This is problematic if records are ever compromised because, unlike a Social Security Number or other unique identifying number, a person cannot change her biometric data.[71] And the many recent security breaches and reports of falsified data show that the government and private sector can

---

Secure Communities by the Numbers: An Analysis of Demographics and Due Process, at p.4, Chief Justice Earl Warren Institute on Law and Social Policy, UC Berkeley School of Law (Oct. 2011), *available at* www.law.berkeley.edu/files/Secure_Communities_by_the_Numbers.pdf.

[67] The Automated Targeting System (ATS), which assigns everyone who crosses United States borders, a computer-generated 'risk assessment' score. Data collected by ATS is "stored for 15 years, even for individuals who have not been flagged as a threat or potential risk." *See* Shana Dines, "Interim Report on the Automated Targeting System: Documents Released through EFF's FOIA Efforts," *EFF.org* (Summer 2009), https://www.eff.org/pages/interim-report-autom. Under ATS, individuals have no way to access information about their "risk assessment" scores or to correct any false information about them. *See* "Lawsuit Demands Answers About Government's Secret 'Risk Assessment' Scores," *EFF* (Dec. 19, 2006), https://www.eff.org/press/archives/2006/12/19.

[68] *See, e.g.,* G.W. Schulz & Andrew Becker, "Finding Meaning In Suspicious Activity Reports," *NPR* (Sept. 7, 2011), http://www.npr.org/2011/09/07/140237086/finding-meaning-in-suspicious-activity-reports; ACLU, *More About Suspicious Activity Reporting* (June 29, 2010), http://www.aclu.org/spy-files/more-about-suspicious-activity-reporting.

[69] *See, e.g.,* Robert Smith, "Julia Shearson tells how a weekend trip to Canada became 5-year fight for rights," *The Plain Dealer* (June 4, 2011), available at http://blog.cleveland.com/metro/2011/06/julia_shearson_tells_how_a_wee.html (describing how Executive Director of the Cleveland Council on American-Islamic Relations (CAIR) ended up on an FBI terrorist watchlist and her struggle to correct inaccuracies in her government files).

[70] *See* "Legal requirements to provide your SSN," *Social Security Online*, http://ssa-custhelp.ssa.gov/app/answers/detail/a_id/78/~/legal-requirements-to-provide-your-ssn.

[71] Records could be compromised in several ways. For example, faceprints are stored as algorithms rather than images. These algorithms could be changed within the database such that when a person tries to use her biometric to identify herself, the database doesn't recognize her or thinks she's someone else.

never fully protect against these kinds of data losses.[72] Data standardization also increases the ability of government and the private sector to locate and track a given person throughout her life.

And finally, extensive data retention periods[73] can lead to further problems; data that may be less identifying today, such as a photograph of a large crowd or political protest, could become more identifiable in the future as technology improves.

However, advanced biometrics like face recognition create additional concerns because the data may be collected in public without a person's knowledge. For example, the addition of crowd and security camera photographs into NGI means that anyone could end up in the database—even if they're not involved in a crime—by just happening to be in the wrong place at the wrong time, by fitting a stereotype that some in society have decided is a threat, or by, for example, engaging in suspect activities such as political protest in areas rife with cameras.[74] Given the FBI's history of misuse of data gathered on people during former FBI director J. Edgar Hoover's tenure[75] and the years following September 11, 2001,[76]—data collection and misuse based on religious beliefs, race, ethnicity and political leanings—Americans have good reason to be concerned about expanding government biometrics databases to include face recognition technology.

Technical issues specific to facial recognition make its use worrisome for Americans. For example, facial recognition's accuracy is strongly dependent on consistent lighting

---

[72] *See, e.g.,* David Stout and Tom Zeller Jr., "Vast Data Cache About Veterans Is Stolen," *N.Y. Times* (May 23, 2006), available at https://www.nytimes.com/2006/05/23/washington/23identity.html; *see also* European Parliament News, *MEPs question Commission over problems with biometric passports* (Apr. 19, 2012) (noting that "In France 500,000 to 1 million of the 6.5 million biometric passports in circulation are estimated to be false, having been obtained on the basis of fraudulent documents.") *available at* http://www.europarl.europa.eu/news/en/headlines/content/20120413STO42897/html/MEPs-question-Commission-over-problems-with-biometric-passports. *See also* discussion of KLIK app hack and Alessandro Acquisti's work supra n. 64.

[73] Biometric records stored in IDENT are retained for 75 years or until the statute of limitations for all criminal violations has expired. DHS, *Privacy Impact Assessment (PIA) for the Automated Biometric Identification System (IDENT)* (Jul. 31, 2006), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_ident_final.pdf. Civil fingerprints stored in IAFIS are not destroyed until "the individual reaches 75 years of age," and criminal fingerprints are not destroyed until "the individual reaches 99 years of age." FBI, *Privacy Impact Assessment for the Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purpose—Channeling* (May 5, 2008), http://www.fbi.gov/foia/privacy-impact-assessments/firs-iafis.

[74] For example, in Lower Manhattan, where the Occupy protests started, the New York Police Department has installed as many as 3,000 security cameras. *See* Noah Shachtman, "NYC Is Getting a New High-Tech Defense Perimeter. Let's Hope It Works," *Wired* (Apr. 21, 2008), http://www.wired.com/politics/security/magazine/16-05/ff_manhattansecurity.

[75] *See generally* Tim Weiner, *Enemies: A History of the FBI* (2012).

[76] *See*, *e.g.,* DOJ, Office of Inspector General (OIG), *A Review of the Federal Bureau of Investigation's Use of National Security Letters*, Special Report (March 2007); DOJ, OIG, *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006,* Special Report*,* (March 2008); DOJ, OIG, *A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records* (January 2010).

conditions and angles of view.[77] It may be less accurate with certain ethnicities and with large age discrepancies (for example, if a person is compared against a photo taken of himself when he was ten years younger). These issues can lead to a high rate of false positives—when, for example, the system falsely identifies someone as the perpetrator of a crime or as having overstayed their visa. In a 2009 New York University report on facial recognition, the researchers noted that facial recognition "performs rather poorly in more complex attempts to identify individuals who do not voluntarily self-identify . . . Specifically, the "face in the crowd" scenario, in which a face is picked out from a crowd in an uncontrolled environment."[78] The researchers concluded the challenges in controlling face imaging conditions and the lack of variation in faces over large populations of people make it unlikely that an accurate face recognition system will become an "operational reality for the foreseeable future."[79]

Some have also suggested the false-positive risk inherent in large facial recognition databases could result in even greater racial profiling by disproportionately shifting the burden of identification onto certain ethnicities.[80] This can alter the traditional presumption of innocence in criminal cases by placing more of a burden on the defendant to show he is *not* who the system identifies him to be. And this is true even if a face recognition system such as NGI offers several results for a search instead of one, because each of the people identified could be brought in for questioning, even if he or she was not involved in the crime. In light of this, German Federal Data Protection Commissioner Peter Schaar has noted that false positives in facial recognition systems pose a large problem for democratic societies: "in the event of a genuine hunt, [they] render innocent people suspects for a time, create a need for justification on their part and make further checks by the authorities unavoidable."[81]

---

[77] Face recognition technologies perform well when all the photographs are taken with similar lighting and shot from a frontal perspective (like a mug shot). However, with different lighting, shadows, different backgrounds, different poses or expressions, or as a person ages, the error rates are significant. See, e.g., P. Jonathon Phillips, et al., "An Introduction to the Good, the Bad, & the Ugly Face Recognition: Challenge Problem," *National Institute of Standards & Testing* (Dec. 2011), available at www.nist.gov/itl/iad/ig/upload/05771424.pdf *(*noting only 15% accuracy for face image pairs that are "difficult to match"). Security researcher Bruce Schneier has noted that even a 90% accurate system "will sound a million false alarms for every real terrorist" and that it is "unlikely that terrorists will pose for crisp, clear photos." Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World,* 190 (2003).

[78] Lucas D. Introna & Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, p. 3, N.Y.U. (April 2009), available at http://www.nyu.edu/ccpr/pubs/Niss_04.08.09.pdf.

[79] *Id*. at 47. In layman's terms, this means that because so many people within a given population look alike, the probability that any facial recognition system will regularly misidentify people becomes much higher as the data set (the population of people you are checking against) gets larger.

[80] *Id*. at 45-46.

[81] *Id*. at 37.

Legal Protections for Privacy in Biometric Data

Face recognition implicates important Constitutional values, including privacy, free speech and association, and the right to be free from unlawful searches and seizures. If the government starts regularly collecting and indexing public photographs—or obtains similar data from private companies—this would have a chilling effect on Americans' willingness to engage in public debate and to associate with others who's values, religion or political views may be considered questionable. And yet the fact that face images can be captured without a detention and in public, or may be uploaded voluntarily to a third party such as Facebook, or may be collected and stored by private security firms and data aggregators, presents significant challenges in applying Constitutional protections.

The Fourth Amendment

The Fourth Amendment's prohibition of unreasonable searches and seizures presents a baseline protection for governmental biometrics collection in the United States.[82] Although there are significant exceptions to Fourth Amendment protections that may make it difficult to map to biometric collection such as facial recognition,[83] a recent Supreme Court case, *U.S. v. Jones*,[84] and a few other cases[85] show that courts are

[82] The Supreme Court has noted that the collection of biometrics like fingerprints has some Fourth Amendment protection, *see Davis v. Mississippi*, 394 U.S. 721, 723-24 (1969) (excluding from evidence fingerprints obtained during an illegal detention), however, the Court has declined to define the boundaries of that protection and suggested in dicta that because "[f]ingerprinting involves none of the probing into an individual's private life and thoughts that marks an interrogation or search[,]" perhaps that protection is limited. *Id.* at 727. Courts have found greater protection in the collection of biological material that "can reveal a host of private medical facts about an [individual]," finding the collection "intrudes upon expectations of privacy that society has long recognized as reasonable." S*kinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 617 (1989).

[83] For example, in each of the key Supreme Court cases to address collection of biometrics or biological material, the legal analysis hinged in large part on the detention required to obtain the biometric data or on "a meaningful interference with [one's] possessory interest in his bodily fluids." *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 618 n.4 (1989). However, biometrics such as face prints can be obtained without an initial detention and without the subject's knowledge while the subject is in a public place. Several cases have held that suspects have no legitimate expectation of privacy in biological material obtained under similar circumstances, *See* Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 Calif. L. Rev. 721, 736 n.63 and accompanying text (2007) (citing cases), or in discarded or abandoned material (such as garbage) or evidence in public view, making Fourth Amendment protection for face prints more tenuous. See, e.g., *California v. Greenwood*, 486 U.S. 35 (1988) (no reasonable expectation of privacy in garbage left on the street); *California v. Ciraolo*, 476 U.S. 207 (1986) (no expectation of privacy in backyard that can be viewed from a plane flying above); Elizabeth Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 Nw. U. L. Rev. 857, 863-64 (2006) (distinguishing cases where courts have found a "meaningful interference with an individual's possessory interests" from cases where "suspects 'knowingly expose' items to public view").

[84] 565 U.S. ____ (2012).

[85] *See, e.g.*, *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) (holding email users have the same reasonable expectation of privacy in their stored email as they do in their phone calls and postal mail); *Montana State Fund v. Simms*, 270 P.3d 64 (Mont. 2012) (in concurring, two justices applied *US v. Jones*, finding the State Fund's "admitted practice of tracking, monitoring, and videotaping workers' compensation claimants as they go about their daily lives" implicated constitutional rights despite the fact that the videotaping occurred in public. The two justices further noted "Montanans do not reasonably expect that

concerned about mass collection of identifying information—even collection of information revealed to the public or a third party—and are trying to identify solutions.

Cases like *Jones* suggest support for the premise that although we may tacitly consent to someone noticing our face or our movements when we walk around in public, it is unreasonable to assume that consent extends to our data being collected and retained in a database, to be subject to repeated searches for the rest of our lives. This is buttressed by important privacy research showing that even though people voluntarily share a significant amount of information about themselves with others online, they still consider much of this information to be private in that they don't expect it to be shared outside of the networks they designate.[86]

In *United States v. Jones*,[87] nine justices held that a GPS device planted on a car without a warrant and used to track a suspect's movements constantly for 28 days violated the Fourth Amendment. For five of the justices, a person's expectation of privacy in not having his movements tracked constantly—even in public—was an important factor in determining the outcome of the case.[88]

Justice Sotomayor would have gone even further, questioning the continued validity of the third-party doctrine (holding that people lack a reasonable expectation of privacy in data such as bank records that they share with a third-party such as the bank).[89] She also recognized that:

> [a]wareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse.[90]

She questioned whether "people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[91]

---

state government, in its unfettered discretion and without a warrant, is recording and aggregating their everyday activities and public movements in a manner which enables the State to ascertain and catalog their political and religious beliefs, their sexual habits, and other private aspects of identity." *Id.* at 71).

[86] danah boyd, *The Future of Privacy: How Privacy Norms Can Inform Regulation*, Oct. 29, 2010, available at http://www.danah.org/papers/talks/2010/PrivacyGenerations.html

[87] 565 U.S. ____ (2012).

[88] *Id.* (slip op. at 2-3) (Sotomayor, J. concurring); *Id.* (slip op. at 9–12) (Alito, J., concurring).

[89] *See also United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010); *Montana State Fund v. Simms*, 270 P.3d 64 (Mont. 2012).

[90] *United States v. Jones,* 132 S. Ct. 945 (Sotomayor, J. concurring), 956; *see also NAACP v. Alabama*, 357 U.S. 449 (1958) (holding that requiring NAACP to disclose membership lists to the government would violate due process and a right to "associate freely with others").

[91] *Id.*

The fact that several members of the Court were willing to reexamine the reasonable expectation of privacy test[92] in light of newly intrusive technology could prove important for future legal challenges to biometrics collection. And some of the questions posed by the justices, both during oral argument and in their various opinions, could be used as models for establishing greater protections for data like facial recognition that is both shared with a third party such as Facebook and gathered in public.[93]

Other Laws May Provide Only Limited Protection to Face Recognition Data Collected by Government and the Private Sector

Privacy Act

The federal Privacy Act[94] "regulates the collection, maintenance, use, and dissemination of information about individuals by federal agencies . . . [and] authorizes civil suits by individuals . . . whose Privacy Act rights are infringed."[95] Although it applies to "personally identified information" collected by the government and gives citizens a way of gaining access to records and requesting their amendment, it has significant exceptions that minimize its effectiveness in actually protecting Americans' privacy rights. For example, it does not offer a remedy for "constitutional claims arising from alleged wrongs covered by the Privacy Act."[96] And law enforcement exemptions that allow agencies to shield criminal justice records from Privacy Act protections[97] make it unlikely it would offer any meaningful protections against face recognition data collection.

Stored Communications Act

The Stored Communications Act,[98] a law passed in 1986, would likely apply to protect face recognition-ready photographs and underlying face print data because it addresses voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by or in storage with third-party service providers like

---

[92] See *Katz v. United States*, 389 U. S. 347, 361 (1967) (Harlan, J., concurring).

[93] Recently, privacy law scholars proposed several ways that Fourth Amendment doctrine could evolve in the wake of *Jones*. *See* www.usvjones.com. Susan Freiwald, who submitted the winning proposal, identified a four-factor test that incorporated factors the Supreme Court and appellate courts already identified. *See* Susan Freiwald, "The Four Factor Test," http://usvjones.com/2012/06/04/the-four-factor-test/ (noting that this four factor test "identifies when a surveillance method intrudes on Fourth Amendment rights and requires heightened judicial oversight to protect against abuse." These factors include whether the surveillance is *hidden* (the target is unaware of it), whether it is *intrusive* (offering access to "things people consider private"), *continuous*, and *indiscriminate* (gathering up "more information than necessary to establish guilt"). These factors could apply to restrict the collection of photographs taken from a hidden security camera that is always on and includes facial recognition.

[94] 5 U.S.C. §552a.

[95] *Jimenez v. Exec. Office for United States Attys.*, 764 F. Supp. 2d 174, 183 (D.D.C. 2011) (citing *Wilson v. Libby*, 535 F.3d 697, 707 (D.C. Cir. 2008)).

[96] *Id*. at 183.

[97] *See e.g.,* 28 C.F.R. § 16.81(a)(4) & (b)(3) (exempting from Privacy Act records maintained in US attorney criminal files).

[98] 18 U.S.C. §§ 2701–2712.

Facebook and Google.[99] However, because the definition of communications and content of communications was written to apply to more traditional oral or written communications,[100] it is unclear how the Act would map to the underlying face print data within a photograph, and whether the government would be required to obtain a warrant or some lesser legal process prior to requesting a copy of this data.[101]

FTC Act

The Federal Trade Commission Act[102] gives the FTC some power to investigate and seek relief for practices that are "unfair" and "deceptive."[103] A trade practice is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits to consumers or competition."[104] A trade practice is "deceptive" if it involves a "material representation, omission or practice that is likely to mislead a consumer acting reasonably in the circumstances, to the consumer's detriment."[105]

The FTC has settled several actions related to privacy in social media or web search that could show how the FTC might address an action related to collection of face recognition data.[106] However, FTC actions are limited, and, unlike court-developed law, the standards for determining whether a trade practice is unfair or deceptive area hazy. In addition, the FTC has so far failed to address the Electronic Privacy Information Center's complaint related to Facebook's face recognition program, despite the fact that it was filed over a year ago.[107] Further, commentators and media regularly recognize that the lack of universal privacy laws in the United States and the limited powers allotted to the FTC to regulate privacy issues, mean that companies have little incentive to change their practices.[108]

---

[99] *Id.* at §2703.

[100] *See* EFF, "Content of Communications," *EFF Internet Law Treatise,* https://ilt.eff.org/index.php/Privacy:_Data_Terminology# Content_of_Communications.

[101] For further discussion of the Stored Communications Act*, see* EFF, "Privacy: Stored Communications Act," *EFF Internet Law Treatise*, https://ilt.eff.org/index.php/Privacy:_Stored_Communications_Act.

[102] 15 U.S.C. §§ 41-58.

[103] *See* 15 U.S.C. § 45 (more commonly known as Section 5 of the FTCA) which declares "unfair or deceptive acts or practices in or affecting commerce" to be unlawful.

[104] 15 U.S.C. § 45(n).

[105] *See* Fed. Trade Comm'n, FTC Policy Statement on Deception, Letter from Fed. Trade Comm'n to Hon. John D. Dingell, Chairman, H. Comm. On Energy and Commerce (Oct. 14, 1983), http://www.ftc.gov/bcp/policystmt/addecept.htm ("Deception Statement").

[106] *See* Julianne Pepitone, "Facebook settles FTC charges over 2009 privacy breaches," *CNN.com* (Nov. 29, 2011) http://money.cnn.com/2011/11/29/technology/facebook_settlement/index.htm; FTC, "FTC Gives Final Approval to Settlement with Google over Buzz Rollout" (Oct. 24, 2011) http://www.ftc.gov/opa/2011/10/buzz.shtm.

[107] *See* EPIC, "Complaint: In re Facebook and the Facial Identification of Users," (June 10, 2011) https://epic.org/privacy/facebook/facebook_and_facial_recognitio.html#complaint.

[108] *See, e.g.,* Ryan Singel, "FTC's $22M Privacy Settlement With Google Is Just Puppet Waving," *Wired Threat Level Blog* (July 10, 2012) http://www.wired.com/threatlevel/2012/07/ftc-google-fine/ (noting that even the FTC's proposed $22.5 million fine to Google for violating the Google Buzz consent decree did not prevent the company from combining all user data).

State Laws[109]

Three states—Illinois, Texas and Washington—have so far implemented laws that expressly apply to biometrics collection. While these laws have some holes, some of their protections could be used as models for federal legislation.

Illinois's law[110] applies to private entities and requires them to notify an individual in writing and obtain a written release before collecting the individual's biometric information, including "face geometry." Entities must disclose "purpose and length of term for which [the] biometric information is being collected, stored, and used," and may further not disclose a collected biometric without the individual's consent, unless the disclosure is required by law. Because this is a state law, it only applies to transactions in Illinois. However, as a state populated with almost 13 million people, Illinois residents could use this law to enforce changes that would likely affect the rest of the country. The law creates private right of action in encourage residents to pursue their own remedies against violations of the law, but with no agency designated to enforce compliance, it does not appear that the law has had much effect so far.

Texas' law[111] similarly regulates collection and use of biometric data, including "face geometry" & prohibits the collection of an individual's biometric data for a commercial purpose without first informing that individual and obtaining her consent. The law does not permit transfers of biometric data for any purpose other than: (1) to identify a deceased or missing individual if that individual previously consented to such identification; (2) for a transaction upon an individual's request or authorization; or (3) to disclose the data pursuant to a state or federal statute or for a law enforcement purpose pursuant to a warrant. Similar to the Illinois law, it creates private right of action for enforcement. It also allows the state Attorney General to bring an action for damages. However, it doesn't appear the Attorney General or any private citizen has yet brought an enforcement action under the law, despite the fact that a base-level reading of the statute would suggest it applies to Facebook's opt-out system.

Washington has had a law regulating biometric drivers' licenses since 2004,[112] which was recently updated to apply to face recognition.[113] The changes, which go into effect this summer, limit the purposes for which face recognition may be used,[114] set standards for

---

[109] Special thanks to EFF Intern Yana Welinder for help with this section on state laws. *See* Yana Welinder, *A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks*, (working paper) (July 16, 2012) *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2109108.

[110] 740 Ill. Comp. Stat. 14/5.

[111] Tex. Bus. & Com. Code Ann. § 503.001.

[112] Chris Ingalls, "State shuts down successful crime-fighting tool," *King5.com* (Sept. 12, 2011) http://www.king5.com/news/investigators/Facial-recognition-program-shutdown--129663433.html.

[113] *See* Rev. Code. Wash. § 46.20.037 (revised by Substitute Senate Bill 6150, to take effect in 2012).

[114] *Id.* Sec. 1 ("Any facial recognition matching system selected by the department must be used only to verify the identity of an applicant for or holder of a driver's license to determine whether the person has been issued a driver's license, permit, or identicard under a different name or names.")

the accuracy of the system and security of the data,[115] provide for a notice requirement,[116] and clarify the legal process required for state and federal law enforcement to access the data.[117] The new version of the statute also includes a reporting requirement.[118] However, where the old version of the law created a voluntary biometrics system for licenses in Washington, the new version appears to remove this voluntariness language.

California may also be worth looking at when considering different protections for biometrics data, especially given how proposed biometrics bills have fared in the state legislature. California has no law specifically protecting biometrics but California's strong constitutional privacy rights,[119] which also apply against private companies, could offer some protections for abuse of those rights. Since 1998, the California legislature has introduced several bills that would directly regulate biometrics collection. However, due in part to industry pushback, none of these laws has moved out of the legislature. Most recently, Senate Bill 761, which would require a company that collects or uses "sensitive information," including biometric data, to allow users to opt-out of its collection, use, and storage, has faced stiff opposition from technology companies and their trade organizations.[120]

The lack of robust protections at the state level makes it even more important for the federal government to consider legislation to prevent improper biometrics collection and search.

Proposals for Change

The over-collection of biometrics has become a real concern, but there are still opportunities—both technological and legal—for change.

Given the current uncertainty of Fourth Amendment jurisprudence in the context of biometrics and the fact that biometrics capabilities are undergoing "dramatic technological change,"[121] legislative action could be a good solution to curb the over-collection and over-use of biometrics in society today and in the future. If so, the federal government's response to two seminal wiretapping cases in the late 60s could be used as

---

[115] *Id.* Sec. 2.

[116] *Id.* Sec. 3, 5 (notice "must address how the facial recognition matching system works, all ways in which the department may use results from the facial recognition matching system, how an investigation based on results from the facial recognition matching system would be conducted, and a person's right to appeal any determinations made under this chapter").

[117] *Id.* Sec. 4 (face recognition data "[m]ay only be disclosed [to state and local law enforcement] when authorized by a court order; [and m]ay only be disclosed to a federal government agency if specifically required under federal law").

[118] *Id.*

[119] Cal. Const. Art 1, sec. 1.

[120] *See* Opp'n Letter to Sen. Lowenthal (Apr. 27, 2011), *available at* http://static.arstechnica.com/oppositionletter.pdf.

[121] *Jones*, 565 U.S. ____, (slip op. at 13) (Alito, J., concurring).

a model.[122] In the wake of *Katz v. United States*[123] and *New York v. Berger*,[124] the federal government enacted the Wiretap Act,[125] which laid out specific rules that govern federal wiretapping, including the evidence necessary to obtain a wiretap order, limits on a wiretap's duration, reporting requirements, and a notice provision.[126] Since then, law enforcement's ability to wiretap a suspect's phone or electronic device has been governed primarily by statute rather than Constitutional case law.

Congress could also look to the Video Privacy Protection Act (VPPA),[127] enacted in 1988, which prohibits the "wrongful disclosure of video tape rental or sale records" or "similar audio-visual materials," requires a warrant before a video service provider may disclose personally identifiable information to law enforcement, and includes a civil remedies enforcement provision.

If legislation or regulations are proposed in the biometrics context, the following principles should be considered to protect privacy and security. These principles are based in part on key provisions of the Wiretap Act and VPPA and in part on the Fair Information Practice Principles (FIPPs), an internationally recognized set of privacy protecting principles.[128]

Limit the Collection of Biometrics—The collection of biometrics should be limited to the minimum necessary to achieve the government's stated purpose. For example, collecting more than one biometric from a given person is unnecessary in many situations. Similarly, the government's acquisition of biometrics from sources other than the individual to populate a database should be limited. For example, the government should not obtain biometrics en masse to populate its criminal databases from sources such as state DMV records, where the biometric was originally acquired for a non-criminal purpose, or from crowd photos or data collected by the private sector. Techniques should

---

[122] In Justice Alito's concurrence in *Jones*, he specifically referenced post-*Katz* wiretap laws and called out for legislative action, noting "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative." *Id*. (slip op. at 11, 13) (Alito, J., concurring).

[123] 389 U.S. 347 (1967).

[124] 388 U.S. 41 (1967). *Berger* was unique in that it struck down a state wiretapping law as facially unconstitutional. In striking down the law, the Court laid out specific principles that would make a future wiretapping statute constitutional under the Fourth Amendment.

[125] 18 U. S. C. §§2510–2522.

[126] *See, e.g.*, Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 851-52 (2004).

[127] 18 U.S.C. § 2710.

[128] *See* Privacy Act of 1974, 5 U.S.C. § 552a (2010). *See also* Organization for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) available at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html. The full version of the FIPPs as used by DHS includes eight principles: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. *See* Hugo Teufel III, Chief Privacy Officer, DHS, Mem. No. 2008-01, Privacy Policy Guidance Memorandum (Dec. 29, 2008), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf. *See also Fair Information Practice Principles*, FTC, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last modified June 25, 2007).

also be employed to avoid over-collection of face prints (such as from security cameras or crowd photos) by, for example, scrubbing the images of faces that are not central to an investigation.

Define Clear Rules on the Legal Process Required for Collection—Each type of biometric should be subject to clear rules on when it may be collected and which specific legal process—such as a warrant based on probable cause—is required prior to collection. Collection and retention should be specifically disallowed without legal process unless the collection falls under a few very limited and defined exceptions. For example, clear rules should be defined to govern when law enforcement or similar agencies may collect biometrics revealed to the public, such as a face print.

Limit the Amount and Type of Data Stored and Retained—For biometrics such as a face print that can reveal much more information about a person than his or her identity, rules should be set to limit the amount of data stored. Retention periods should be defined by statute and should be limited to no longer than necessary to achieve the goals of the program. Data that is deemed to be "safe" from a privacy perspective today could become highly identifying tomorrow. For example, a data set that includes crowd images could become much more identifying as technology improves. Similarly, data that was separate and siloed or unjoinable today might be easily joinable tomorrow. For this reason retention should be limited, and there should be clear and simple methods for a person to request removal of his or her biometric from the system if, for example, the person has been acquitted or is no longer under investigation.[129]

Limit the Combination of More than One Biometric in a Single Database—Different biometric data sources should be stored in separate databases. If biometrics need to be combined, that should happen on an ephemeral basis for a particular investigation. Similarly, biometric data should not be stored together with non-biometric contextual data that would increase the scope of a privacy invasion or the harm that would result if a data breach occurred. For example, combining facial recognition technology from public cameras with license plate information increases the potential for tracking and surveillance. This should be avoided or limited to specific individual investigations.

Define Clear Rules for Use and Sharing—Biometrics collected for one purpose should not be used for another purpose. For example, face prints collected for use in a criminal context should not automatically be used or shared with an agency to identify a person in an immigration context. Similarly, photos taken in a non-criminal context, such as for a driver's license, should not be shared with law enforcement without proper legal process. For private sector databases, users should be required to consent or opt-in to any face recognition system.

[129] For example, in *S. and Marper v. United Kingdom*, the European Court of Human Rights held that retaining cellular samples and DNA and fingerprint profiles of people acquitted or people who have had their charges dropped violated Article 8 of the European Convention on Human Rights. *S. and Marper. v. United Kingdom*, App. Nos. 30562/04 and 30566/04, 48 Eur. H.R. Rep. 50, 77, 86 (2009).

Enact Robust Security Procedures to Avoid Data Compromise—Because biometrics are immutable, data compromise is especially problematic. Using traditional security procedures, such as basic access controls that require strong passwords and exclude unauthorized users, as well as encrypting data transmitted throughout the system, is paramount. However security procedures specific to biometrics should also be enacted to protect the data. For example, data should be anonymized or stored separate from personal biographical information. Strategies should also be employed at the outset to counter data compromise after the fact and to prevent digital copies of biometrics. Biometric encryption[130] or "hashing" protocols that introduce controllable distortions into the biometric before matching can reduce the risk of problems later. The distortion parameters can easily be changed to make it technically difficult to recover the original privacy-sensitive data from the distorted data, should the data ever be breached or compromised.[131]

Mandate Notice Procedures—Because of the real risk that face prints will be collected without their knowledge, rules should define clear notice requirements to alert people to the fact that a face print has been collected. The notice provision should also make clear how long the biometric will be stored and how to request its removal from the database.

Define and Standardize Audit Trails and Accountability Throughout the System—All database transactions, including biometric input, access to and searches of the system, data transmission, etc. should be logged and recorded in a way that assures accountability. Privacy and security impact assessments, including independent certification of device design and accuracy, should be conducted regularly.

Ensure Independent Oversight—government entities that collect or use biometrics must be subject to meaningful oversight from an independent entity. Individuals whose biometrics are compromised, whether by the government or the private sector should have a strong and meaningful private right of action.

Conclusion

Face recognition and its accompanying privacy concerns are not going away. Given this, it is imperative that government act now to limit unnecessary biometrics collection; instill proper protections on data collection, transfer, and search; ensure accountability; mandate independent oversight; require appropriate legal process before government collection; and define clear rules for data sharing at all levels. This is important to preserve the democratic and constitutional values that are bedrock to American society.

Thank you once again for the invitation to testify today. I am happy to respond to your questions.

---

[130] *See, e.g.,* Information and Privacy Commissioner, Ontario, Canada, *Privacy-Protective Facial Recognition: Biometric Encryption—Proof of Concept* (Nov. 2010), available at www.ipc.on.ca/images/Resources/pbd-olg-facial-recog.pdf.

[131] *See, e.g.,* Center for Unified Biometrics and Sensors, "Cancellable Biometrics," SUNY Buffalo, http://www.cubs.buffalo.edu/cancellable.shtml (last visited Mar. 15, 2012).