ELECTRONIC FRONTIER FOUNDATION

United States House Committee on
Oversight and Government Reform

Hearing on Law Enforcement's Use of Facial Recognition Technology

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

March 22, 2017

For further information, please contact Jennifer Lynch at
jlynch@eff.org *or* 415.436.9333x136

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee:

Thank you very much for the opportunity to discuss facial recognition technology. My name is Jennifer Lynch, and I am a senior staff attorney with the Electronic Frontier Foundation (EFF), a non-profit, member-supported, public-interest organization that works to protect privacy and civil liberties in new technologies.[1]

I. Introduction

Since my 2012 testimony on face recognition before the Senate Subcommittee on Privacy, Technology, and the Law,[2] face recognition technology has advanced significantly. Now, law enforcement officers can use mobile devices to capture face recognition-ready photographs of people they stop on the street; surveillance cameras boast real-time face scanning and identification capabilities; and the FBI has access to hundreds of millions of face recognition images of law-abiding Americans.

However, the adoption of face recognition technologies like these has occurred without meaningful oversight, without proper accuracy testing of the systems as they are actually used in the field, and without the enactment of legal protections to prevent their misuse.

This has led to the development of unproven, inaccurate systems that will impinge on constitutional rights and disproportionately impact people of color.

The FBI's Interstate Photo System and FACE Services Unit exemplify these problems. The minimal testing conducted by the Bureau showed the IPS was incapable of accurate identification at least 15% of the time. This has real-world impact; an inaccurate system will implicate people for crimes they didn't commit, forcing them to try to prove their innocence and shifting the traditional burden of proof away from the government.

This threat will likely disproportionately impact people of color. Face recognition misidentifies African Americans and ethnic minorities, young people, and women at

---

[1] Founded in 1990, EFF represents the interests of tens of thousands of dues-paying members and the public in both court cases and broader policy debates surrounding the application of law in the digital age. EFF is particularly concerned with protecting privacy at a time when technological advances have resulted in increased surveillance by the government and actively encourages and challenges government and the courts to support privacy and safeguard individual autonomy as emerging technologies become prevalent in society.

[2] *See Testimony of Jennifer Lynch to the Senate Committee on the Judiciary Subcommittee on Privacy, Technology, and the Law* (July 18, 2012) *available at* https://www.eff.org/files/filenode/jenniferlynch_eff-senate-testimony-face_recognition.pdf.

higher rates than whites, older people, and men, respectively.[3] Due to years of well-documented, racially-biased police practices, all criminal databases—including mug shot databases—include a disproportionate number of African Americans, Latinos, and immigrants.[4] These two facts mean people of color will likely shoulder exponentially more of the burden of the Interstate Photo System's inaccuracies than whites.

Despite these known challenges, FBI has for years also failed to be transparent about its use of face recognition technology. It took seven years to update its Privacy Impact Assessment for the IPS and didn't release one until a year after its system was fully operational. And the public had no idea how many images were accessible to its FACE Services Unit until last year's scathing Government Accountability Office report revealed the Bureau could access nearly 412 million images—most of which were taken for non-criminal reasons like obtaining a driver license or a passport.

Without transparency, accountability, and proper security protocols in place, face recognition systems—like many other searchable databases of information available to law enforcement—may be subject to misuse. This misuse has already occurred in other contexts. For example, in 2010, Immigration and Customs Enforcement enlisted local police officers to use license plate readers to gather information about gun-show customers.[5] In Florida in 2011, more than 100 officers accessed driver and vehicle information for a female Florida state trooper after she pulled over a Miami police officer for speeding.[6] And a state audit that same year of law enforcement access to driver information in Minnesota revealed "half of all law-enforcement personnel in Minnesota

---

[3] *See* B. F. Klare, M. J. Burge, J. C. Klontz, R. W. Vorder Bruegge and A. K. Jain, "Face Recognition Performance: Role of Demographic Information," in,*IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1789-1801, (Dec. 2012). http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6327355&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Ficp.jsp%3Farnumber%3D6327355. *See also* Clare Garvie & Jonathan Frankle, "Facial-Recognition Software Might Have a Racial Bias Problem," *The Atlantic* (Apr. 7, 2016) http://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/.

[4] *See* NAACP, Criminal Justice Fact Sheet (2009) *available at* https://donate.naacp.org/pages/criminal-justice-fact-sheet.

[5] Devlin Barrett, *Gun-Show Customers' License Plates Come under Scrutiny*, Wall St. J. (Oct. 2, 2016), http://www.wsj.com/articles/gun-show-customers-license-plates-come-under-scrutiny-1475451302.

[6] Dave Elias, *Deputy fired for misusing driver's license database*, NBC2 (April 24, 2014) http://www.nbc-2.com/story/25334275/deputy-fired-for-improperly-accessing-info-about-governor-nbc2-anchors-others.

had misused driving records."[7]

Americans should not be forced to submit to criminal face recognition searches merely because they want to drive a car. They shouldn't have to worry their data will be misused by unethical government officials with unchecked access to face recognition databases. And they shouldn't have to fear that their every move will be tracked if face recognition is linked to the networks of surveillance cameras that blanket many cities.

But without meaningful legal protections, this is where we may be headed. Without laws in place, it could be relatively easy for the government and private companies to amass databases of images of all Americans and use those databases to identify and track people in real time as they move from place to place throughout their daily lives. As researchers at Georgetown discovered last year, 1 out of 2 Americans is already in a face recognition database accessible to law enforcement.[8]

As this Committee noted in its excellent 2016 report on law enforcement use of cell-site simulators, "advances in emerging surveillance technologies" like face recognition "require careful evaluation to ensure their use is consistent with the protections afforded under the First and Fourth Amendments to the U.S. Constitution."[9] And, just as with cell-site simulators, transparency and accountability are critical to ensuring that face recognition's use not only comports with Constitutional protections but also preserves democratic values.

Justice Alito noted in his concurring opinion in *United States v. Jones* that, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."[10] Just as this Committee found with cell-site simulators, the use of face recognition must be limited. I urge the Committee to introduce legislation to do just that.

---

[7] Chris Francescani, *License to Spy,* Medium (Dec. 1, 2014), https://medium.com/backchannel/the-drive-to-spy-80c4f85b4335.

[8] Clare Garvie, et al., *The Perpetual Line-Up*, Georgetown Law Center on Privacy & Technology (Oct. 18, 2016) https://www.perpetuallineup.org/jurisdiction/florida.

[9] *Law Enforcement Use of Cell Site Simulation Technologies: Privacy Concerns and Recommendations*, House Committee on Oversight & Government Reform (Dec. 19, 2016) *available at* https://oversight.house.gov/wp-content/uploads/2016/12/THE-FINAL-bipartisan-cell-site-simulator-report.pdf.

[10] 565 U.S. 400, 429 (2012) (Alito, J., concurring).

II. FBI's Next Generation Identification Database and the Interstate Photo System

The FBI's Next Generation Identification system (NGI) is a massive biometric database that includes fingerprints, iris scans, and palm prints collected from individuals not just during arrests, but also from millions of Americans and others for non-criminal reasons like background checks, state licensing requirements, and immigration, The Interstate Photo System (IPS) is the part of NGI that contains images like mug shots and non-criminal photographs that are searchable through face recognition. Each of these biometric identifiers is linked to personal, biographic, and identifying information, and, where possible, each file includes multiple biometric identifiers. FBI has designed NGI to be able to expand in the future as needed to include "emerging biometrics," such as footprint and hand geometry, gait recognition, and others.[11]

NGI incorporates both criminal and civil records. NGI's criminal file includes records on people arrested at the local, state, and federal level as well as biometric data taken from crime scenes and data on missing and unidentified persons. NGI's civil repository stores biometric and biographic data collected from members of the military and those applying for immigration benefits. It also includes biometric data collected as part of a background check or state licensing requirement for many types of jobs, including licensing to be a dentist, accountant, teacher, geologist, realtor, lawyer or even an optometrist. Since 1953, all jobs with the federal government have also required a fingerprint check, no matter the salary range or level of responsibility.[12]

---

[11] FBI, *Next Generation Identification*, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi; FBI, *Biometric Center of Excellence*, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/biometric-center-of-excellence/modalities.

[12] *See, e.g.,* Dental Board of Cal., *Fingerprint Requirement for License Renewal* (2016) *available at* http://www.dbc.ca.gov/licensees/fingerprint_faq.shtml#q1; Texas State Board of Public Accountancy, *New Fingerprinting Process for CPA Exam Applicants* (August 1, 2014) https://www.tsbpa.texas.gov/info/2014072801.html; Wisc. Dept of Public Instruction, *Completing the Fingerprint Requirement* (August 1, 2013) http://dpi.wi.gov/tepdl/licensing/fingerprint; *See* Cal. Dept. of Consumer Affairs Bd for Professional Engineers, Land Surveyors, and Geologists, *Fingerprinting FAQ's* (2012) http://www.bpelsg.ca.gov/applicants/fingerprinting_faqs.shtml; State of New Jersey Dept. of Banking & Insurance, *Real Estate License Candidate Fingerprinting* (February 1, 2015) http://www.state.nj.us/dobi/division_rec/licensing/fingerprint.html*;* The State Bar of Cal., *Moral Character Determination Instructions* (2016) https://www.calbarxap.com/applications/calbar/info/moral_character.html#fingerprints; Cal. Dept. of Consumer Affairs Bd of Optometry,

As of February 2017, NGI included nearly 73 million records in the criminal repository and over 53 million records in the civil repository.[13] By December 2015, it also already contained nearly 30 million civil and criminal photographs searchable through face recognition.[14]

The states have been very involved in the development of the NGI database. NGI includes more than 20 million civil and criminal images received directly from at least six states, including California, Louisiana, Michigan, New York, Texas, and Virginia. And it appears five additional states—Florida, Maryland, Maine, New Mexico, and Arkansas—can send search requests directly to the NGI database. As of December 2015, FBI was working with eight more states to grant them access to NGI, and an additional 24 states were also interested.[15]

In 2015, FBI announced that for the first time it would link almost all of the non-criminal data in NGI with criminal data as a "single identity record."[16] This means that now, if a person submits fingerprints as part of their job search, those prints will be searched continuously along with the criminal prints thousands of times a day[17] for any crime by more than 20,000 law enforcement agencies across the country and around the world.[18]

FBI has said—for now—that it is keeping non-criminal photographs in the IPS separate

---

Fingerprint Requirement for License Renewal (June 21, 2010) http://www.optometry.ca.gov/faqs/fingerprint.shtml#q1.

[13] *See* FBI, *Next Generation Identification (NGI) Monthly Fact Sheet* (February 2017) *available at* https://www.fbi.gov/file-repository/ngi-monthly-fact-sheet/view (hereinafter "February 2017 NGI Monthly Fact Sheet").

[14] Government Accountability Office, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy*, 46, GAO-16-267 (May 2016) http://www.gao.gov/assets/680/677098.pdf (hereinafter "GAO Report").

[15] GAO Report at 13. The Report does not list these remaining states.

[16] FBI, *Next Generation Identification (NGI)—Retention and Searching of Noncriminal Justice Fingerprint Submissions* (Feb. 20, 2015) https://www.fbi.gov/foia/privacy-impact-assessments/next-generation-identification-ngi-retention-and-searching-of-noncriminal-justice-fingerprint-submissions.

[17] *See* Adam Vrankulj, *NGI: A closer look at the FBI's billion-dollar biometric program* (November 4, 2013) *available at* http://www.biometricupdate.com/201311/ngi-a-closer-look-at-the-fbis-billion-dollar-biometric-program.

[18] *See* February 2017 NGI Monthly Fact Sheet.

from criminal photographs.[19] However, if a person is ever arrested for any crime—even for something as minor as blocking a street as part of a First Amendment-protected protest—their non-criminal photographs will be combined with their criminal record and will become fair game for the same face recognition searches associated with any criminal investigation.[20] As of December 2015, over eight million civil records were also included in the criminal repository.[21]

III. FBI Access to External Face Recognition Databases

The public did not begin to learn about FBI's ability to access external face recognition databases until the Bureau issued a Privacy Impact Assessment (PIA) for its Facial Analysis, Comparison, and Evaluation (FACE) Services Unit in May 2015. However, the full scope of that access was not revealed until the Government Accountability Office (GAO) issued its scathing report on FBI use of face recognition over a year later.

The GAO Report disclosed for the first time that FBI had access to over 400 million face recognition images—hundreds of millions more than journalists and privacy advocates had been able to estimate before that. According to the GAO Report, the FACE Services unit not only has access to FBI's Next Generation Identification (NGI) face recognition database of nearly 30 million civil and criminal mug shot photos, it also has access to the State Department's Visa and Passport databases, the Defense Department's biometric database, and the drivers license databases of at least 16 states. Totaling 411.9 million images, this is an unprecedented number of photographs, and most of these were collected from Americans and foreigners under civil and not criminal circumstances.

Under agreements we have never seen between the FBI and its state and federal partners, the FBI may search these civil photos whenever it is trying to find a suspect in a crime. And FACE Services has been searching its external partner databases a lot; from August 2011 through December 2015, the FBI requested nearly 215,000 searches of external

---

[19] *See* Ernest J. Babcock, Senior Component Official for Privacy, FBI, *Privacy Impact Assessment for the Next Generation Identification (NGI) Interstate Photo System* (September 2015) *available at* https://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system.

[20] *See, e.g.*, AZ Rev. Stat. § 13-2906 (Obstructing a highway or other public thoroughfare; classification).

[21] *See* FBI, *Next Generation Identification (NGI) Monthly Fact Sheet* (December 2015) *available at* https://web.archive.org/web/20160331181001/https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi/december-2015-ngi-fact-sheet.pdf (hereinafter "December 2015 NGI Monthly Fact Sheet"). The FBI's current Monthly Fact Sheet omits this information. *Compare* February 2017 NGI Monthly Fact Sheet.

partners' databases.[22] FACE Services also receives thousands of requests from those partners for its services; since the beginning of the current fiscal year, it received more than 28,000 requests for face recognition-related searches.[23]

IV. For Years, FBI Failed to Produce Basic Information about NGI and its Use of Face Recognition as Required by Federal Law

Despite going live with NGI in increments since at least 2008, FBI failed to release basic information about its system, including mandatory PIAs and a new System of Records Notice (SORN), that would have informed the public on what data the FBI has been collecting and how that data is being used and protected.[24]

In failing to issue timely PIAs for the Interstate Photo System and the work of the FBI's FACE Services Unit, as well as a SORN for the entire NGI system, FBI also failed to comply with key provisions of both the Privacy Act of 1974 and the E-Government Act of 2002.[25]

PIAs are an important check against the encroachment on privacy by the government. They allow the public to see how new programs and technology used by the government affect their privacy and assess whether the government has done enough to mitigate the privacy risks. As the DOJ's own guidelines on PIAs explain, "[t]he PIA also . . . helps promote trust between the public and the Department by increasing transparency of the Department's systems and missions."[26] The are also mandatory.[27]

PIAs should also be conducted during the development of any new system "with sufficient lead time to permit final Departmental approval and public website posting on

---

[22] GAO Report at 10.

[23] *See* February 2017 NGI Monthly Fact Sheet.

[24] EFF and other organizations called for years on FBI to release more information about NGI and how it impacts people's privacy. *See, e.g.*, *Testimony of Jennifer Lynch to the Senate Committee on the Judiciary Subcommittee on Privacy, Technology, and the Law* (July 18, 2012) *available at* https://www.eff.org/document/testimony-jennifer-lynch-senate-committee-judiciary-subcommittee-privacy-technology-and-law; Letter to Attorney General Holder re. Privacy Issues with FBI's Next Generation Identification Database (June 24, 2014) *available at* https://www.eff.org/document/letter-attorney-general-holder-re-privacy-issues-fbis-next-generation-identification.

[25] 5 U.S.C. § 552a; Public Law 107–347 (2002).

[26] OPCL DOJ, Privacy Impact Assessments Official Guidance, 3 (Rev. March 2012) *available at* https://www.justice.gov/opcl/docs/2012-doj-pia-manual.pdf.

[27] *Id*. (footnotes omitted).

or before the commencement of any system operation (including before any testing or piloting.)"[28]

Despite these requirements, FBI began developing one of NGI's most important capabilities—face recognition—by at least 2008, and it issued a PIA for the IPS that same year. However, it didn't update that PIA until late 2015—a full year after the entire Interstate Photo System was online and fully operational and as many as seven years after FBI first started incorporating face recognition-compatible photographs into NGI.[29] Before FBI issued the new PIA, it had already conducted over 100,000 searches of the database.[30]

FBI also failed to produce a System of Records Notice (SORN) for the NGI system until 2016.[31] The Privacy Act requires all federal agencies to produce a SORN for any system that collects and uses Americans' personal information.[32] Those SORNs must describe exactly what data is collected and how it is being used and protected. But for years FBI skirted the Privacy Act—instead of producing a new System of Records Notice (SORN) for NGI, it relied on an outdated SORN from 1999 describing its legacy IAFIS database[33]—a database that only included fingerprints and non-searchable photographs. Even FBI now admits that NGI contains nine "enhancements" that make it fundamentally different from the original IAFIS database that it replaces.[34]

The GAO Report specifically faulted FBI for amassing, using, and sharing its face recognition technologies without ever explaining the privacy implications of its actions to the public. As GAO noted, the whole point of a PIA is to give the public notice of the privacy implications of data collection programs and to ensure that privacy protections

---

[28] *Id.* at 4.

[29] FBI, *Privacy Impact Assessment for the Next Generation Identification (NGI) Interstate Photo System* (Sept. 2015) https://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system (hereinafter "2015 FBI Interstate Photo System PIA"); *see also* Tim Cushing, *FBI Rolls Out Biometric Database On Schedule, Accompanying Privacy Impact Assessment Still Nowhere To Be Found* (September 16, 2014) https://www.techdirt.com/articles/20140916/09090628533/fbi-rolls-out-biometric-database-schedule-accompanying-privacy-impact-assessment-still-nowhere-to-be-found.shtml.

[30] GAO Report at 49.

[31] 81 Fed. Reg. 27283 (May 5, 2016).

[32] 5 U.S.C. § 552a(e)(4).

[33] FBI, 64 FR 52343 (09-28-99) https://www.fbi.gov/foia/privacy-act/64-fr-52343.

[34] Proposed FBI NGI SORN.

are built into the system from the start. FBI failed to do this.

V. NGI is Inaccurate, Impinges on First and Fourth Amendment Rights, and Disproportionately Impacts People of Color

A. FBI Has Failed to Address the Problem of Face Recognition Inaccuracy

FBI has done little to ensure its face recognition search results (which the Bureau calls "investigative leads") do not implicate innocent people. According to the GAO report and FBI's responses to EFF's Freedom of Information Act requests, FBI has conducted only very limited testing to ensure the accuracy of NGI's face recognition capabilities. And it has not taken any steps to determine whether the face recognition systems of its external partners—states and other federal agencies—are sufficiently accurate to prevent innocent people from being identified as criminal suspects.

FBI admits its system is inaccurate, noting in its PIA for the Interstate Photo System that IPS "may not be sufficiently reliable to accurately locate other photos of the same identity, resulting in an increased percentage of misidentifications."[35] However, FBI has disclaimed responsibility for accuracy in its face recognition system, stating that "[t]he candidate list is an investigative lead not an identification."[36] Because the system is designed to provide a ranked list of candidates, FBI has stated NGI never actually makes a "positive identification," and "therefore, there is no false positive rate."[37] In fact, FBI only ensures that "the candidate will be returned in the top 50 candidates" 85 percent of the time "when the true candidate exists in the gallery."[38] It is unclear what happens when the "true candidate" does *not* exist in the gallery, however—does NGI still return possible matches? Could those people then be subject to criminal investigation for no other reason than that a computer thought their face was mathematically similar to a suspect's?

The GAO Report criticizes FBI's cavalier attitude regarding false positives, noting that "reporting a detection rate without reporting the accompanying false positive rate presents an incomplete view of the system's accuracy."[39] The Report also notes that

---

[35] 2015 FBI Interstate Photo System PIA.

[36] *See* Jennifer Lynch, *FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year*, and accompanying documents. The Bureau has also noted that because "this is an investigative search and caveats will be prevalent on the return detailing that the [non-FBI] agency is responsible for determining the identity of the subject, there should be NO legal issues." *Id*.

[37] *Id.*

[38] *Id.*

[39] GAO Report at 27.

FBI's stated detection rate may not represent operational reality because FBI only conducted testing on a limited subset of images and failed to conduct additional testing as the size of the database increased. FBI also has never tested to determine detection rates where the size of the responsive candidate pool is reduced to a number below 50.[40]

When false positives represent real people who may become suspects in a criminal investigation, the number of false positives a system generates is especially important.[41] But technical issues endemic to all facial recognition systems mean false positives will continue to be a common problem for the foreseeable future.

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, when photographs that are compared to one another contain different lighting, shadows, different backgrounds, or different poses or expressions, the error rates can be significant.[42] Face recognition is also less accurate with large age discrepancies (for example, if people are compared against a photo taken of themselves when they were ten years younger).

Face recognition is also extremely challenging at low resolutions.[43] EFF learned through documents FBI released in response to our 2012 FOIA request that the median resolution of images submitted through an Interstate Photo System pilot program was "well-below" the recommended resolution of 3/4 of a megapixel (in comparison, newer iPhone cameras are capable of twelve megapixel resolution[44]).[45] Another FBI document released to EFF

---

[40] GAO Report at 26.

[41] 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).

[42] *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").

[43] *See, e.g.*, Min-Chun Yang, et al., Recognition at a Long Distance: Very Low Resolution Face Recognition and Hallucination, IEEE 2015 International Conference on Biometrics, 237-242 (May 2015).

[44] *See* Apple, *Compare iPhone Models* (2017) *available at* https://www.apple.com/iphone/compare/.

noted that because "the trend for the quality of data received by the customer is lower and lower quality, specific research and development plans for low quality submission accuracy improvement is highly desirable."

Finally, Face recognition performs worse overall as the size of the data set (the population of people you are checking against) increases, in part because so many people within a given population look similar to one another. At 30 million searchable photos so far, the FBI's face recognition system constitutes a very large data set.

Given all of these challenges, identifying an unknown face in a crowd using NGI's database of face images would still be particularly challenging.[46]

Using humans to perform the final suspect identification from a group of photos provided by the system does not solve these accuracy problems. Research has shown that, without specialized training, humans may be worse at identification than a computer algorithm. And that is especially true when the person is someone they don't already know or someone of a race or ethnicity different from their own.[47]

---

[45] *See* Jennifer Lynch, *FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year*, EFF (April 14, 2014) and accompanying documents at https://www.eff.org/deeplinks/2014/04/fbi-plans-have-52-million-photos-its-ngi-face-recognition-database-next-year.

[46] A 2009 New York University report concluded that, given these challenges, it is unlikely that face recognition systems with high accuracy rates under these conditions will become an "operational reality for the foreseeable future." Lucas D. Introna & Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, p. 3, N.Y.U. (April 2009) http://www.nyu.edu/ccpr/pubs/Niss_04.08.09.pdf. Recently, Russian developers announced that their system, called FindFace, could identify a person on the street with about 70% accuracy if that person had a social media profile. However, it is unclear at what resolution and distance the probe photos were taken and how many images of each person were available to compare the probe photos against (more photographs taken from different angles and under different lighting conditions could increase the probability of a match). *See, e.g.*, Ben Guarino, *Russia's new FindFace app identifies strangers in a crowd with 70 percent accuracy*, Wash. Post (May 18, 2016) https://www.washingtonpost.com/news/morning-mix/wp/2016/05/18/russias-new-findface-app-identifies-strangers-in-a-crowd-with-70-percent-accuracy/.

[47] *See* Clare Garvie, et al., *The Perpetual Line-Up*, Georgetown Law Center on Privacy & Technology, 49 (Oct. 18, 2016)(internal citations omitted).

B. The Scope of NGI and FBI's Use of Face Recognition Are Still Unclear

Although FBI finally produced a proposed SORN for NGI in Summer 2016, there is still a lot the public does not know about the system and FBI's plans for its future evolution. For example, a Request for Proposals FBI released in 2015 indicated the agency planned to allow law enforcement officers to use mobile devices to collect face recognition data out in the field and submit that data directly to NGI.[48] As we have seen with state and local agencies that have already begun using such devices, officers may use mobile biometric tools in ways that push the limits of and in some cases directly contradict constitutional law. For example, in San Diego, where officers from multiple agencies use mobile devices to photograph people right on the street and immediately upload those images to a shared face recognition database, officers have pressured citizens to consent to having their picture taken.[49] Regional law enforcement policy has also allowed collection based on First-Amendment protected activities like an "individual's political, religious, or social views, associations or activities" as long as that collection is limited to "instances directly related to criminal conduct or activity."[50]

From FBI's past publications related to NGI, including the Request for Proposals, the PIA for the Interstate Photo System, and the SORN for NGI, it is unclear whether FBI would retain the images collected with mobile devices in the NGI database. If it does, this would directly contradict 2012 congressional testimony where an FBI official said "[o]nly criminal mug shot photos are used to populate the national repository."[51] A photograph taken in the field before someone is arrested is not a "mug shot."

FBI may also decide to use NGI in other ways. A 2011 Memorandum of Understanding (MOU) between Hawaii and FBI shows that the government has considered "permit[ting] photo submissions independent of arrests."[52] It is not clear from the document, what

---

[48] *See* Jennifer Lynch, *FBI Plans to Populate its Massive Face Recognition Database with Photographs Taken in the Field*, EFF (Sept. 18, 2015) https://www.eff.org/deeplinks/2015/09/little-fanfare-fbi-ramps-biometrics-programs-yet-again-part-2.

[49] *See* Jennifer Lynch and David Maas, *San Diego Gets in Your Face With New Mobile Identification System*, EFF (Nov. 7, 2013) https://www.eff.org/deeplinks/2013/11/san-diego-gets-your-face-new-mobile-identification-system.

[50] *Id*.

[51] Jerome M. Pender, Deputy Assistant Director, Criminal Justice Information Services Division, FBI, *Statement Before the Senate Judiciary Committee, Subcommittee on Privacy, Technology, and the Law* (July 18, 2012) https://www.fbi.gov/news/testimony/what-facial-recognition-technology-means-for-privacy-and-civil-liberties.

[52] *Hawaii Memorandum of Understanding (MOU) with FBI for Face Recognition Photos*

types of photos this could include. The Bureau also indicated in a 2010 presentation that it wants to use NGI to track people's movements to and from "critical events" like political rallies, to identify people in "public datasets," to "conduct[] automated surveillance at lookout locations," and to identify "unknown persons of interest" from photographs.[53] This suggests FBI wants to be able to search and identify people in photos of crowds and in pictures posted on social media sites—even if the people in those photos haven't been arrested for or suspected of a crime.

FBI's 2015 PIA for the Interstate Photo System and its proposed SORN leave open this possibility that FBI may plan to incorporate crowd or social media photos into NGI in the future. The PIA notes that NGI's "unsolved photo file" contains photographs of "unknown subjects," and the SORN notes the system includes "biometric data" that has been "retrieved from locations, property, or persons associated with criminal or national security investigations."[54] Because criminal investigations may occur in virtual as well as physical locations, this loophole seems to allow FBI to include images collected from security cameras, social media accounts, and other similar sources.

Finally, at some point in the future, FBI may also attempt to populate NGI with millions of other non-criminal photographs. The GAO Report notes FBI's FACE Services unit already has access to the IPS, the State Department's Visa and Passport databases, the Defense Department's biometric database, and the drivers license databases of at least 16 states.[55] However, the combined 412 million images in these databases may not even represent the full scope of FBI access to face recognition data today. When GAO's Report first went to press, it noted that FBI officials had stated the Bureau was in negotiations with 18 additional states to obtain access to their drivers license databases.[56] This information was kept out of later versions of the Report, so it is unclear where these negotiations stand today. The later version of the report also indicates Florida does not share its drivers license data with FBI, but Georgetown's recent report on law enforcement access to state face recognition databases contradicts this; Georgetown

---

(November 20, 2011) *available at* https://www.eff.org/document/hawaii-memorandum-understanding-mou-fbi-face-recognition-photos.

[53] *See* Richard W. Vorder Bruegge, *Facial Recognition and Identification Initiatives*, Federal Bureau of Investigation 5 (2010) *available at* https://www.eff.org/document/fbi-facial-recognition-initiatives-presentation-2010-biometrics-conference.

[54] Proposed FBI NGI SORN.

[55] GAO Report at 47-48.

[56] *Compare* map of states sharing data with FACE Services on page 51 of the GAO Report with map available in original version of Report, available here: https://www.eff.org/deeplinks/2016/06/fbi-can-search-400-million-face-recognition-photos.

found FBI field offices in Florida can search all drivers license and ID photos in the state.[57]

C. Face Recognition Uniquely Impacts Civil Liberties

These uses of NGI would clearly impact Fourth Amendment rights and First Amendment-protected activities and would chill speech. They could also violate a key provision of the Privacy Act designed to prevent data collection on First Amendment protected activities.[58] The addition of crowd and security camera photographs and DMV photographs into NGI would mean that anyone could end up in the database without their knowledge—even if they're not suspected of 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 public spaces rife with cameras. Given FBI's history of misuse of data gathered on people during former FBI director J. Edgar Hoover's tenure[59] and during the years following September 11, 2001,[60]—data collection and misuse based on religious beliefs, race, ethnicity, and political leanings—Americans have good reason to be concerned about expanding government face recognition databases.

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 individuals cannot take precautions to prevent the collection of their image. Face recognition allows for covert, remote, and mass capture and identification of

---

[57] Clare Garvie, et al., *The Perpetual Line-Up*, Georgetown Law Center on Privacy & Technology (Oct. 18, 2016) https://www.perpetuallineup.org/jurisdiction/florida.

[58] *See* 5 U.S.C. 552a(e)(7) (forbidding agencies from maintaining "records describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity").

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

[60] *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).

images[61]—and the photos that may end up in a database could include not just a person's face but also how she is dressed and possibly whom she is with.

Face recognition and the accumulation of easily identifiable photographs implicate important free speech and freedom of association rights and values under the First Amendment, especially because face-identifying photographs of crowds or political protests can be captured in public without individuals' knowledge or online and through public and semi-public social media sites.

Law enforcement has already used face recognition technology at political protests. Marketing materials from the social media monitoring company Geofeedia bragged that, during the protests surrounding death of Freddie Gray, the Baltimore Police Department ran social media photos against a facial recognition database to identify protesters and arrest them.[62]

Government surveillance such as this has a very real chilling effect on Americans' willingness to engage in public debate and to associate with others whose values, religion, or political views may be considered different from their own. For example, researchers have long studied the "spiral of silence"— the significant chilling effect on an individual's willingness to publicly disclose political views when they believe their views differ from the majority.[63] Last year, research on Facebook users documented the silencing effect of participants' dissenting opinions in the wake of widespread knowledge of government surveillance—participants were far less likely to express negative views of government surveillance on Facebook when they perceived those views were outside the norm.[64]

In 2013, a large study of Muslims in New York and New Jersey found a significant

---

[61] *See* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 Minn. L. Rev. 2, 407, 415 (Dec. 2012).

[62] *Baltimore County Police Department and Geofeedia Partner to Protect the Public During Freddie Gray Riots*, *available at* https://www.aclunc.org/docs/20161011_geofeedia_baltimore_case_study.pdf.

[63] *See, e.g.*, Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, Journalism & Mass Comm. Quarterly 2016, Vol. 93(2) 296–311, *available at* http://journals.sagepub.com/doi/pdf/10.1177/1077699016630255.

[64] *See* Karen Turner, "Mass Surveillance Silences Minority Opinions, According to Study," Wash. Post (March 28, 2016) https://www.washingtonpost.com/news/the-switch/wp/2016/03/28/mass-surveillance-silences-minority-opinions-according-to-study/?utm_term=.6d51b07dbb33.

chilling effect on First-Amendment protected activities due to police surveillance in Muslim communities.[65] Specifically, people were less inclined to attend mosques they thought were under government surveillance or to engage in religious practices in public or even to dress or grow their hair in ways that might subject them to surveillance based on their religion. People were also less likely to engage with others in their community they didn't know for fear that person would either be a government informant or a radical. Parents discouraged their children from participating in Muslim social, religious, or political movements. Business owners took conscious steps to mute political discussion by turning off Al-Jazeera in their stores. And activists self-censored their comments on Facebook.[66]

These examples show the very real risks to First Amendment protected speech and activities from excessive government surveillance—especially when that speech represents the minority viewpoint. While we don't yet appear to be at point where face recognition is being used broadly to monitor the public, we are at a stage where the government is building out the databases to make that monitoring possible. It is important to place meaningful checks on government use of face recognition now before we reach a point of no return.

D. NGI Disproportionately Impacts People of Color

The false-positive risks discussed above could also disproportionately impact African Americans and other people of color.[67] Research—including research jointly conducted by one of FBI's senior photographic technologists—found that face recognition misidentified African Americans and ethnic minorities, young people, and women at higher rates than whites, older people, and men, respectively.[68] Due to years of well-

---

[65] Diala Shamas & Nermeen Arastu, *Mapping Muslims: NYPD Spying and its Impact on American Muslims* (March 11, 2013) http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf.

[66] *Id*.

[67] Nellie Bowles, *'I think my blackness is interfering': does facial recognition show racial bias?*, The Guardian (April 8, 2016) *available at* https://www.theguardian.com/technology/2016/apr/08/facial-recognition-technology-racial-bias-police.

[68] *See* B. F. Klare, M. J. Burge, J. C. Klontz, R. W. Vorder Bruegge and A. K. Jain, "Face Recognition Performance: Role of Demographic Information," in,*IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1789-1801 (Dec. 2012) http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6327355&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Ficp.jsp%3Farnumber%3D6327355. *See also* Clare Garvie & Jonathan Frankle, "Facial-Recognition Software Might Have a Racial Bias Problem," *The Atlantic* (Apr. 7, 2016)

documented racially-biased police practices, all criminal databases—including mugshot databases—include a disproportionate number of African Americans, Latinos, and immigrants.[69] These two facts mean people of color will likely shoulder exponentially more of the burden of NGI's inaccuracies than whites.

False positives can alter the traditional presumption of innocence in criminal cases by placing more of a burden on suspects and defendants to show they are *not* who the system identifies them to be. 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 there is nothing else linking them to the crime. Former German Federal Data Protection Commissioner Peter Schaar has noted that false positives in facial recognition systems pose a large problem for democratic societies. "[I]n 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."[70]

NGI's face recognition accuracy problems will also unfairly impact African American and minority job seekers who must submit to background checks. Employers regularly rely on FBI's data when conducting background checks. If job seekers' faces are matched mistakenly to mug shots in the criminal database, they could be denied employment through no fault of their own. And even if job seekers are properly matched to a criminal mug shot, minority job seekers will be disproportionately impacted due to the notorious unreliability of FBI records as a whole. At least 50 percent of FBI's arrest records fail to include information on the final disposition of the case—whether a person was convicted, acquitted, or if charges against them were dropped.[71] Because at least 30 percent of

---

http://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/.

[69] *See* NAACP, Criminal Justice Fact Sheet (2009) *available at* https://donate.naacp.org/pages/criminal-justice-fact-sheet.

[70] Lucas D. Introna & Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, 37, N.Y.U. (April 2009) http://www.nyu.edu/ccpr/pubs/Niss_04.08.09.pdf.

[71] *See* Madeline Neighly & Maurice Emsellem, *WANTED: Accurate FBI Background Checks for Employment*, National Employment Law Project (July 2013) *available at* http://www.nelp.org/content/uploads/2015/03/Report-Wanted-Accurate-FBI-Background-Checks-Employment.pdf. *See also* Ellen Nakashima, "FBI Wants to Exempt Its Huge Fingerprint and Photo Database from Privacy Protections," *Washington Post* (June 30, 2016) https://www.washingtonpost.com/world/national-security/fbi-wants-to-exempt-its-huge-fingerprint-and-photo-database-from-privacy-protections/2016/05/31/6c1cda04-244b-11e6-8690-f14ca9de2972_story.html (noting

people arrested are never charged with or convicted of any crime, this means a high percentage of the FBI's records incorrectly indicate a link to crime. If these arrest records are not updated with final disposition information, hundreds of thousands of Americans searching for jobs could be prejudiced and lose work. And due to disproportionately high arrest rates, this uniquely impacts people of color.

E. FBI Has Failed to Ensure Face Recognition Data are Protected from Internal and External Security Breaches

The many recent security breaches, email hacks, and reports of falsified data—including biometric data—show that the government must have extremely rigorous security measures and audit systems in place to protect against data loss. Just this past year, news media were consumed with stories of hacks into email and government systems, including into United States political organizations and online voter registration databases in Illinois and Arizona.[72] In 2015, hackers were able to steal sensitive data stored in Office of Personnel Management databases on more than 25 million people.[73] These data included biometric information as well as addresses, health and financial history, travel data, and data on people's friends and neighbors. It has been described as the largest cyberattack into United States government systems, and even FBI Director James Comey called the breach "a very big deal."[74] More than anything, though, these breaches exposed the vulnerabilities in government systems to the public—vulnerabilities that the United States government appears to have known for almost two decades might exist.[75]

---

that, according to FBI, "43 percent of all federal arrests and 52 percent of all state arrests — or 51 percent of all arrests in NGI — lack final dispositions").

[72] *See, e.g.,* Tracy Connor, et al., *U.S. Publicly Blames Russian Government for Hacking*, NBC News (Oct. 7, 2016) http://www.nbcnews.com/news/us-news/u-s-publicly-blames-russian-government-hacking-n662066.

[73] Julie Hirschfeld Davis, "Hacking of Government Computers Exposed 21.5 Million People," *N.Y. Times* (July 9, 2015) http://www.nytimes.com/2015/07/10/ us/office-of-personnel-management-hackers-got-data-of-millions.html. *See also, e.g.,* David Stout and Tom Zeller Jr., "Vast Data Cache About Veterans Is Stolen," *N.Y. Times* (May 23, 2006), 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.") http://www.europarl.europa.eu/news/en/headlines/content/20120413STO42897/html/MEPs-question-Commission-over-problems-with-biometric-passports.

[74] *Id.*

[75] *Id*.

Vulnerabilities exist from insider threats as well. Past examples of improper and unlawful police use of driver and vehicle data suggest face recognition data will also be misused. For example, in 1998, a Washington, D.C., police officer "pleaded guilty to extortion after looking up the license plates of vehicles near a gay bar and blackmailing the vehicle owners."[76] In 2008, the Virginia State Police used automated license plate readers to scan the plates of all vehicles entering facilities for Palin and Obama rallies.[77] In 2010, Immigration and Customs Enforcement enlisted local police officers to use license plate readers to gather information about gun-show customers.[78] Four Utah police officers were disciplined for misusing a confidential database.[79] Between 2014 and 2015, Florida's Department of Highway Safety and Motor Vehicles reported about 400 cases of improper use of its Driver and Vehicle Information Database.[80] And a 2011 state audit of law enforcement access to driver information in Minnesota revealed "half of all law-enforcement personnel in Minnesota had misused driving records."[81]

Officers may also access data to provide information to others unaffiliated with the police. For example, in 2014, two New York police officers were indicted after they were reportedly paid to tap into a confidential law enforcement database to obtain personal information about potential witnesses.[82] A Phoenix, Arizona officer "gave a woman involved in a drug and gun-trafficking investigation details about stolen cars in exchange

---

[76] Julia Angwin & Jennifer Valentino-DeVries, *New Tracking Frontier: Your License Plates*, Wall St. J. (Sept. 29, 2012), http://online.wsj.com/news/articles/SB10000872396390443995604578004723603576 29.

[77] Letter from First Sergeant Bobbie D. Morris to First Sergeant Alvin D. Blankenship on Division Seven Heat Operations (Mar. 18, 2009), *available at* http://www.thenewspaper.com/rlc/docs/2013/va-alpr.pdf.

[78] Devlin Barrett, *Gun-Show Customers' License Plates Come under Scrutiny*, Wall St. J. (Oct. 2, 2016), http://www.wsj.com/articles/gun-show-customers-license-plates-come-under-scrutiny-1475451302.

[79] Sadie Gurman & Eric Tucker, *Across U.S., Police Officers Abuse Confidential Databases*, Salt Lake Tribune (Sept. 28, 2016) http://www.sltrib.com/home/4407962-155/ap-across-us-police-officers-abuse.

[80] *Id*.

[81] Chris Francescani, *License to Spy,* Medium (Dec. 1, 2014), https://medium.com/backchannel/the-drive-to-spy-80c4f85b4335.

[82] Benjamin Weiser, *2 Former New York Police Officers Misused Database, U.S. Says,* N.Y. Times (Oct. 22, 2014), http://www.nytimes.com/2014/10/23/nyregion/us-accuses-2-former-police-officers-of-abusing-a-confidential-database.html?

for arranging sexual encounters for him."[83] And police have provided license plate data to reporters.[84]

Many of the recorded examples of database misuse involve male officers targeting women. For example, in Florida, an officer breached the driver and vehicle database to "look up a local bank teller he was reportedly flirting with."[85] More than 100 other Florida officers accessed driver and vehicle information for a female Florida state trooper after she pulled over a Miami police officer for speeding.[86] In Ohio, officers looked through the database to find information on an ex-mayor's wife, along with council people and spouses. [87] In Illinois, a police sergeant suspected of murdering two ex-wives used police databases to check up on one of his wives before she disappeared.[88]

It is unclear whether federal agencies have done much in the years before and after the OPM hack to improve the security of their systems. In 2007, the GAO specifically criticized FBI for its poor security practices. GAO found, "[c]ertain information security controls over the critical internal network reviewed were ineffective in protecting the confidentiality, integrity, and availability of information and information resources."[89]

---

[83] Gurman & Tucker, *Across U.S., Police Officers Abuse Confidential Databases.*

[84] Dave Maass, *Mystery Show Debunks License Plate Privacy "Myth*," EFF (June 15, 2015), https://www.eff.org/deeplinks/2015/06/mystery-show-podcast-debunks-license-plate-privacy-myth.

[85] Amy Pavuk, *Law-Enforcer Misuse of Driver Database Soars*, Orlando Sentinel (Jan. 22, 2013) http://articles.orlandosentinel.com/2013-01-22/news/os-law-enforcement-access-databases-20130119_1_law-enforcement-officers-law-enforcers-misuse; *see also* Kim Zetter, *Cops Trolled Driver's License Database for Pic of Hot Colleague*, WIRED (Feb 23, 2012), https://www.wired.com/2012/02/cop-database-abuse/.

[86] Dave Elias, *Deputy Fired for Misusing Driver's License Database*, NBC2 (April 24, 2014) http://www.nbc-2.com/story/25334275/deputy-fired-for-improperly-accessing-info-about-governor-nbc2-anchors-others

[87] Eric Lyttle, *Fairfield County Grand Jury Indicts Two over Misuse of Database for Police*, Columbus Dispatch (April 24, 2015), http://www.dispatch.com/content/stories/local/2015/04/23/sugar-grove-police-indicted.html.

[88] Brad Flora, *What Do the Cops Have on Me?*, Slate (Dec 4, 2007), http://www.slate.com/articles/news_and_politics/explainer/2007/12/what_do_the_cops_have_on_me.html.

[89] Government Accountability Office, Information Security: FBI Needs to Address Weaknesses in Critical Network, GAO-07-368 (April 2007) http://www.gao.gov/new.items/d07368.pdf.

Given this and the fact that FBI intends to retain personal data in NGI for the length of a person's life plus seven years,[90] FBI must do more to explain why it needs to collect so much sensitive biometric and biographic data, why it needs to maintain it for so long, and how it will safeguard the data from the data breaches we know will occur in the future.

VI. Despite the Serious Issues Outlined Above, FBI has Proposed Exempting Face Recognition Data from Key Provisions of the Privacy Act

FBI proposes to exempt much of the NGI database from three key provisions of the Privacy Act: (1) the right to access records maintained on oneself; (2) the right to ensure that those records are maintained accurately and to be able to correct inaccuracies; and (3) the right to know with whom one's data are being shared.

FBI recognizes, as it must, that the Privacy Act not only requires it to maintain accurate records but also to ensure that the information it disseminates to other federal and non-federal agencies is "accurate, complete, timely and relevant."[91] FBI states that it takes this obligation seriously.[92] Nevertheless, FBI recognizes both that a significant percentage of its data is already inaccurate or out of date[93] and that face recognition is not necessarily reliable as an identification tool.[94] This means FBI has already failed to meet its legal duties under the Privacy Act.

FBI's proposed exemptions seek to prevent Americans from ever knowing exactly what data the Bureau maintains on them and shares with other agencies. And, by seeking to remove any judicial remedy, the exemptions attempt to prevent Americans from ensuring that the data the Bureau maintains is "accurate, complete, timely and relevant."

This has real-world consequences. For example, a few years ago, due to notoriously inaccurate and out-of-date immigration and arrest records,[95] approximately 3,600 United

---

[90] *See* Proposed FBI NGI SORN, "RETENTION AND DISPOSAL."

[91] 2015 FBI Interstate Photo System PIA.

[92] FBI & DOJ, Notice of Proposed Rulemaking, 81 Fed. Reg. 27288 (May 5, 2016).

[93] *See* Ellen Nakashima, "FBI Wants to Exempt Its Huge Fingerprint and Photo Database from Privacy Protections," *Washington Post* (June 30, 2016).

[94] 2015 FBI Interstate Photo System PIA.

[95] *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*

States citizens were caught up in the "Secure Communities" program—a program that resulted in detention and deportation for thousands of people.[96] FBI's proposed exemptions would take away the ability for citizens in cases such as these to learn whether the inaccurate records leading to their detention came from the Bureau. The proposed exemptions also seek to remove those citizens' rights to force FBI to correct and update its records.

Given the vast scope of data included in NGI, the impact that inaccuracies in that data would have on Americans' lives, and the possibility FBI and other agencies may use this data—in violation of the Privacy Act—to monitor First Amendment protected activities, FBI should not be allowed to exempt NGI from the Privacy Act.

VII. Proposals for Change

The over-collection of face recognition data 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 face recognition and the fact that the technology is undergoing "dramatic technological change,"[97] legislative action could be a good solution to curb the over-collection and over-use of face recognition data in society, both now and in the future. If so, the federal government's response to two seminal wiretapping cases in the late 60s could be used as a model.[98] In the wake of *Katz v. United States*[99] and *New York v. Berger*,[100] the federal

---

http://www.gao.gov/products/GAO-11-146 (noting errors in USCIS's e-Verify system and difficulties in correcting those errors).

[96] *See, e.g.,* Aarti Kohli, et al. *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.

[97] *United States v. Jones*, 565 U.S. 400, 427 (2012) (Alito, J., concurring).

[98] 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*. at 427-28, 429.

[99] 389 U.S. 347 (1967).

[100] 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.

government enacted the Wiretap Act,[101] which lays out specific rules that govern federal wiretapping, including the evidence necessary to obtain a wiretap order, limits on a wiretap's duration, reporting requirements, a notice provision, and also a suppression remedy that anticipates wiretaps may sometimes be conducted unlawfully.[102] 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),[103] 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 face recognition 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 standards.[104]

Limit the Collection of Data—The collection of face recognition data should be limited to the minimum necessary to achieve the government's stated purpose. For example, the government's acquisition of face recognition from sources other than directly from the individual to populate a database should be limited. The government should not obtain face recognition data 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

---

[101] 18 U. S. C. §§2510–2522.

[102] *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); 18 U.S.C. § 2515.

[103] 18 U.S.C. § 2710.

[104] *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.

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—Face recogntion should be subject to clear rules on when it may be collected and which specific legal processes—such as a warrant based on probable cause—are 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 face recognition images from the general public without their knowledge.

Limit the Amount and Type of Data Stored and Retained—A face print can reveal much more information about a person than his or her identity, so 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, with a high priority placed on deleting data. 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.[105]

Limit the Combination of More than One Biometric in a Single Database—Different biometric data sources should be stored in separate databases. If face recognition needs to be combined with other biometrics, 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, photos taken in a non-criminal context, such as for a drivers license, should not be shared with law enforcement without proper

---

[105] 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).

legal process. Similarly, 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. Face recognition should not be used to identify and track people in real time without a warrant. And private sector databases should be required to obtain user consent before enrolling people into any face recognition system.

Enact Robust Security Procedures to Avoid Data Compromise—Because biometrics cannot be changed, 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[106] 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.[107]

Mandate Notice Procedures—Because of the real risk that face prints will be collected without a person's 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 data 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 face recognition 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 face recognition must be subject to meaningful oversight from an independent entity. Individuals whose data are compromised, whether by the government or the private sector should have a strong and meaningful private right of action.

---

[106] *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.

[107] *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).

VIII. Conclusion

Face recognition and its accompanying privacy and civil liberties concerns are not going away. Given this, it is imperative that government act now to limit unnecessary data collection; instill proper protections on data collection, transfer, and search; ensure accountability; mandate independent oversight; require appropriate legal process before collection and use; 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. I am happy to respond to questions.

Respectfully submitted,

Jennifer Lynch
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
jlynch@eff.org

Committee on Oversight and Government Reform
Witness Disclosure Requirement — "Truth in Testimony"

Pursuant to House Rule XI, clause 2(g)(5) and Committee Rule 16(a), non-governmental witnesses are required to provide the Committee with the information requested below in advance of testifying before the Committee. You may attach additional sheets if you need more space.

Name:

1. Please list any entity you are testifying on behalf of and briefly describe your relationship with these entities.

Name of Entity	Your relationship with the entity
Electronic Frontier Foundation	Senior Staff Attorney

2. Please list any federal grants or contracts (including subgrants or subcontracts) you or the entity or entities listed above have received since January 1, 2015, that are related to the subject of the hearing.

Recipient of the grant or contact (you or entity above)	Grant or Contract Name	Agency	Program	Source	Amount
—	—	—	—	—	—

2. Please list any payments or contracts (including subcontracts) you or the entity or entities listed above have received since January 1, 2015 from a foreign government, that are related to the subject of the hearing.

Recipient of the grant or contact (you or entity above)	Grant or Contract Name	Agency	Program	Source	Amount
—	—	—	—	—	—

I certify that the information above and attached is true and correct to the best of my knowledge.

Signature _____ Date: 3/20/17

JENNIFER LYNCH
Senior Staff Attorney
Electronic Frontier Foundation
815 Eddy St. San Francisco 94109

415 / 436–9333x136
jlynch@eff.org
@lynch_jen

JENNIFER LYNCH—BIOGRAPHY

Jennifer Lynch is a senior staff attorney with the Electronic Frontier Foundation (EFF) and works on privacy and civil liberties issues implicated by new technologies. She writes and speaks frequently on government surveillance programs, and her work has appeared in the Wall Street Journal, the New York Times, and the National Law Journal, among others. Jennifer challenges surveillance technologies like location tracking devices, face recognition, and drones, through the courts and successfully sued the federal government to obtain thousands of pages of previously unpublished drone records. Jennifer also works to promote privacy-protective laws in federal and state legislatures and testified about face recognition and surveillance in the United States Senate and in the California state legislature. She is regularly consulted as an expert on the Fourth Amendment and surveillance by major and technical news media across the country.