epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

FEDERAL BUREAU OF INVESTIGATION

of the

DEPARTMENT OF JUSTICE

Privacy Act of 1974; Systems of Record
Notice of a Modified System of Records Notice

[CPCLO Order No. 002-2016]

Privacy Act of 1974; Implementation
Notice of Proposed Rulemaking

[CPCLO Order No. 003-2016]

July 6, 2016

By notice published May 5, 2016, the Department of Justice's Federal Bureau of Investigation ("FBI") proposes to modify the Fingerprints Identification Record ("FIRS") by renaming the records system the Next Generation Identification ("NGI") System.[1] Additionally, the FBI is modifying the system to "add and clarify the categories of

[1] Notice of Privacy Act System of Records, 81 Fed. Reg. 27,284 (proposed May 5, 2016) [hereinafter NGI SORN]. On June 6, 2016 the comment period for the NGI SORN was extended to July 6, 2016. Notice of a Modified System of Records Notice; Extension of Comment Period, 81 Fed. Reg. 36,350 (June 6, 2016).

individuals and records maintained in NGI, and their associated Routine Uses, as well as updating procedures for individuals to access and contest their records."[2]

By notice published May 5, 2016, the FBI also proposed to exempt the NGI System from several significant provisions of the Privacy Act of 1974.[3] Pursuant to the FBI's notices, the Electronic Privacy Information Center ("EPIC") submits these comments to urge the agency to: (1) adhere to Congress's intent to maintain transparent and secure government recordkeeping systems; (2) provide individuals judicially enforceable rights of notice, access, and correction; and (3) limit the collection and retention of data, especially biometric data.

I. EPIC's Interest

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in preserving privacy safeguards, established by Congress, in the development of information systems operated by the federal government.[4]

EPIC has repeatedly called for increased oversight of NGI. In 2011, 70 organizations, including EPIC, urged the Inspector General of the Department of Justice

[2] NGI SORN.
[3] Notice of Proposed Rulemaking, 81 Fed. Reg. 27,288 (proposed May 5, 2016) [hereinafter NGI NPRM]. On June 6, 2016 the comment period for the NGI NPRM was extended to July 6, 2016. Notice of Proposed Rulemaking; Extension of Comment Period, 81 Fed. Reg. 36,228 (June 6, 2016).
[4] EPIC, *Comments on Docket CPCLO Order No. 006-2012: Proposed Rule: Privacy Act of 1974 Exemptions* (May 18, 2012), https://epic.org/apa/comments/EPIC-DEA-CPCLO-006-2012.pdf; EPIC, *Comments on Docket AAG/A Order Nos. 005-2005 and 006-2005: Concerning Notice to Establish Terrorist Screening Records System* (Sept. 6, 2005), https://epic.org/privacy/airtravel/tsrs_comments090605.html.

to investigate the privacy and civil liberties implications of the FBI's NGI program.[5] In 2014, as NGI neared full operational capacity, EPIC and a coalition of civil liberties groups urged Attorney General Eric Holder to review the NGI program and release an updated Privacy Impact Assessment as a first step to robust review of the program.[6] Since that letter, NGI has gone fully operational with minimal oversight. Last year EPIC called upon Congress to hold a hearing on the FBI's NGI database.[7] Last month, EPIC reiterated its call for a Congressional hearing on NGI with a coalition of 45 organizations.[8]

EPIC has also pursued a series of Freedom of Information Act requests to determine the accuracy and reliability of the NGI records system.[9] As a result of these FOIA requests, EPIC has determined that FBI facial searches returned an incorrect candidate up to 20% of the time.[10]

II. The FBI's NGI Database Maintains a Massive Amount of Personal, Sensitive Information About a Wide Variety of Individuals

According to the SORN, the NGI Database will include detailed, personal information about an expansive array of individuals, many of whom have never been charged with any criminal misconduct. The following categories of records are maintained in the FBI NGI database:

---

[5] Letter from Coalition of Civil Liberties groups to Cynthia A. Schnedar, DOJ Acting Inspector General (Sept. 11, 2011), https://epic.org/privacy/secure_communities/DOJ-S-Comm-Letter.pdf.
[6] Letter from Coalition of Civil Liberties groups to Eric Holder, U.S. Attorney General (June 24, 2014), https://www.privacycoalition.org/Ltr-to-Review-FBI-NGI-Program.pdf.
[7] Letter from EPIC to Chairman Grassley and Ranking Member Leahy of the S. Jud. Comm. (Jan. 9, 2015), https://epic.org/foia/fbi/ngi/EPIC-to-SJC-re-NGI.pdf.
[8] Letter from Coalition Privacy, Transparency, Civil Rights, Human Rights, and Immigrant groups to Senators Grassley and Leahy, and Representatives Goodlatte, Chaffetz, Conyers, and Cummings (June 23, 2016), https://epic.org/privacy/fbi/NGI-Congressional-Oversight-Letter.pdf.
[9] *See, e.g.*, EPIC, *EPIC v. FBI – Next Generation Identification*, http://epic.org/foia/fbi/ngi/.
[10] FBI, *Next Generation Identification (NGI) System Requirements Document*, 244 (Oct. 1, 2010), http://epic.org/foia/fbi/ngi/NGI-System-Requiremets.pdf.

A. criminal fingerprint images with related biographic, biometric, and criminal justice information;
B. civil fingerprint images with related biographic, biometric, and noncriminal justice information;
C. fingerprint images with related biographic, biometric, and event information maintained for the purposes of national security (*e.g.* known or appropriately suspected terrorists);
D. fingerprint images with related biographic, biometric, and event information received from federal government agencies pursuant to the FBI's authority to identify and investigate federal crimes and threats to the national security;
E. fingerprint images with related biographic, biometric and event information received from foreign countries or international organizations pursuant to sharing agreements;
F. Identity History Summary records that contain the criminal justice information associated with criminal fingerprints (*i.e.* "rap sheets") and/or the noncriminal justice information associated with civil fingerprints;
G. a name index pertaining to all individuals whose criminal fingerprint images are maintained in the system (*i.e.* the Interstate Identification Index);
H. biometric images (*e.g.* palm prints, facial images) maintained for criminal, civil, and/or national security purposes;
I. latent fingerprints and palm prints and/or other latent biometric images maintained for criminal and/or national security purposes;
J. unknown facial images and palm prints and/or other unknown biometric images maintained for criminal and/or national security purposes;
K. fingerprint images and/or other biometric images maintained in support of disaster response humanitarian efforts, or similar purposes;
L. fingerprint images with related biographic, biometric, and event information maintained pursuant to an individual's request or consent.[11]

This "related biometric information" includes fingerprints; palmprints; iris data; scars, marks, and tattoos; and voice data.[12] In addition to biometric markers, the related "biographic information" includes corresponding criminal histories (date of arrest and arrest events); mug shots; scars, marks, and tattoo photos; physical characteristics like

[11] NGI SORN at 27,285.
[12] Richard W. Vorder Bruegge, *Facial Recognition and Identification Initiatives*, FED. BUREAU OF INVESTIGATION BIOMETRIC CTR. FOR EXCELLENCE; http://biometrics.org/bc2010/presentations/DOJ/vorder_bruegge-Facial-Recognition-and-Identification-Initiatives.pdf; *see also* FBI, *Fingerprints & other Biometrics: Next Generation Identification*, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi (discussing the iris recognition pilot program).

height, weight, hair color, eye color; aliases;[13] race; sex; country of citizenship; place of birth; employer name and contact information.[14]

The FBI is also proposing to increase the scope of biometric information collection. The FBI's Biometric Center of Excellence (BCOE) is dedicated to "leveraging the potential of newly emerging biometric technology to allow federal government agencies to increase their identity management capabilities."[15] The BCOE is developing and enhancing new biometric technologies including footprint and hand geometry, ear recognition, and gait recognition.[16] These technologies will likely be integrated into the NGI system. The FBI's website states:

> The NGI Program will advance the integration strategies and indexing of additional biometric data that will provide the framework for a future multimodal system that will facilitate biometric fusion identification techniques. The framework will be expandable, scalable, and flexible to accommodate new technologies and biometric standards, and will be interoperable with existing systems.[17]

The increasing types of biometrics and information the FBI is seeking to collect greatly raises the privacy risks of NGI.

---

[13] FBI, *Integrated Automated Fingerprint Identification System*, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis.
[14] FBI, *Technical Specifications Document for the Interstate Photo System Facial Recognition Pilot Project*, 489, 513 (May 2, 2012), http://epic.org/foia/fbi/ngi/IPSFRP-Technical-Specs.pdf.
[15] FBI, *Emerging Biometrics*, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/modalities/emerging-biometrics.
[16] *Id.;* Richard W. Vorder Bruegge, *Facial Recognition and Identification Initiatives*, FED. BUREAU OF INVESTIGATION BIOMETRIC CTR. FOR EXCELLENCE (2010), http://biometrics.org/bc2010/presentations/DOJ/vorder_bruegge-Facial-Recognition-and-Identification-Initiatives.pdf.
[17] FBI-CJIS, *Next Generation Identification*, https://www2.fbi.gov/hq/cjisd/ngi.htm; *see also* FBI, *Capital Asset Summary* (July 20, 2012), https://it-2013.itdashboard.gov/investment/exhibit300/pdf/011-000003457 (stating that new and more accurate biometric identification capabilities are being incorporated incrementally).

III. The FBI's Collection and Retention Policy Regarding Personal, Sensitive Information Exposes Millions to Unnecessary Privacy Risks

The NGI database includes profiles on arrestees and people with records as well as individuals with no connection to the criminal justice system. Increasingly, the FBI is collecting information, including biometric information, for non-criminal reasons and keeping that data well beyond the original need for collection. For example, the FBI's "Rap Back" program collects fingerprints from employees, licensees, and others for ongoing background checks even when the individual has no prior criminal record.[18] The FBI defended the program as a way to eliminate the need for periodic rescreening of the individual and the resubmission of fingerprints.[19] Once the fingerprints are entered into the database, the records are kept by the FBI until individual turns 110, or seven years after their death. Individuals cannot get their records purged unless they have a court order. Additionally, fingerprints and other information are collected from individuals who apply for immigration benefits or commit civil law violations.

a. The FBI's NGI Database Needlessly Exposes Millions to a Potential Data Breach

The over collection of detailed, sensitive information is problematic particularly in light of the rise of government data breaches. Overall, the number of government data breaches has exploded in the last decade, rising from 5,503 in 2006 to 67,168 in 2014.[20]

---

[18] FBI, *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) - Retention and Searching of Noncriminal Justice Fingerprint Submissions*, https://www.fbi.gov/foia/privacy-impact-assessments/next-generation-identification-ngi-retention-and-searching-of-noncriminal-justice-fingerprint-submissions.

[19] FBI, *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) - Retention and Searching of Noncriminal Justice Fingerprint Submissions*, https://www.fbi.gov/foia/privacy-impact-assessments/next-generation-identification-ngi-retention-and-searching-of-noncriminal-justice-fingerprint-submissions.

[20] U.S. Gov't Accountability Office, *Federal Agencies Need to Better Protect Sensitive Data* 4

The 2015 Office of Personnel Management (OPM) data breaches compromised the personal information of 21.5 million people, including 1.8 million people who did not apply for a background check.[21] The OPM breach exposed sensitive information spanning three decades.[22] The personal and sensitive information that was exposed includes an individual's name; date of birth; Social Security Number (SSN); address; social media activity; personal and official email addresses and phone numbers; citizenship, ethnicity and race; employment and educational history; passport, driver's license, and license plate numbers; medical reports; biometric data; photographic images, videotapes, and voice recordings; and "[i]nformation on family members, dependents, relatives, and other personal associations."[23] The fingerprints of 5.6 million people were also stolen in the data breach.[24] This information could be used to blackmail government employees, expose the identities of foreign contacts, and cause serious damage to counterintelligence and national security efforts.[25]

Furthermore, the risk of breach was not unexpected. One year prior to the OPM

(Nov. 17, 2015), http://www.gao.gov/assets/680/673678.pdf.

[21] Dan Goodin, *Call it a "Data Rupture": Hack Hitting OPM Affects 21.5 Million*, ARSTECHNICA (July 9, 2015), http://arstechnica.com/security/2015/07/call-it-a-data-rupture-hack-hitting-opm-affects-21-5- million/.

[22] Andrea Shalal & Matt Spetalnick, *Data Hacked from U.S. Government Dates Back to 1985: U.S. Official*, REUTERS (June 5, 2015), http://www.reuters.com/article/us-cybersecurity-usa-idUSKBN0OL1V320150606.

[23] *Form: SF86*, U.S. GENERAL SERVICES ADMINISTRATION, http://www.gsa.gov/portal/forms/download/116390.

[24] Andrea Peterson, *OPM Says 5.6 Million Fingerprints Stolen in Cyberattack, Five Times as Many as Previously Thought*, WASH. POST (Sep. 23 2015), https://www.washingtonpost.com/news/the- switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/.

[25] *See* Kim Zetter & Andy Greenberg, *Why the OPM Breach is Such a Security and Privacy Debacle*, WIRED (June 11, 2015), http://www.wired.com/2015/06/opm-breach-security-privacy-debacle/.

breach, the Inspector General warned OPM about its privacy and security flaws.[26] Despite this information, OPM did not implement the recommended changes. The extent of the breach could have been mitigated if data minimization policies were put in place. The agency maintained records on individuals as far back at 1985 and unnecessarily put retirees at risk of identity theft.[27]

While the OPM breach compromised the fingerprints of 5.6 million people, the NGI database contains over 30 million photos and associated fingerprints, along with other biometric data, and the database is quickly growing.[28] The increasing aggregation of biometric data in one spot makes the NGI database an enticing target for criminals—especially given the rise of the use of biometrics for secure access and their immutable property. If a Social Security Number is stolen in a breach, one can apply for a new number, and mitigate the interim risk with credit reporting; individuals cannot change their facial features, fingerprints, or other biometric traits. Their security and safety could be compromised for the rest of their lives. As fingerprint and iris scans increasingly replace passwords, there is growing concern that hackers will seek to leverage this information.[29] OPM's remedy, 3 years of identity theft services,[30] is insufficient to guard

---

[26] *Final Audit Report*, U.S. OFFICE OF PERSONNEL MANAGEMENT OFFICE OF THE INSPECTOR GENERAL OFFICE OF AUDITS (2014), https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf.

[27] Andrea Shalal & Matt Spetalnick, *Data Hacked from U.S. Government Dates Back to 1985: U.S. Official*, REUTERS (June 5, 2015), http://www.reuters.com/article/us-cybersecurity-usa-idUSKBN0OL1V320150606.

[28] U.S. Gov't Accountability Office, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy* (May 2016), http://www.gao.gov/products/GAO-16-267 [hereinafter "GAO Face Recognition Report"].

[29] Andrea Peterson, *OPM Says 5.6 Million Fingerprints Stolen in Cyberattack, Five Times as Many as Previously Thought*, WASH. POST (Sep. 23 2015),

against the potential for misuse of biometric data if it is compromised.

Given the recent surge in government data breaches, the vast amount of sensitive information contained in the NGI Database faces significant risk of compromise. According to a recent report by the U.S. Government Accountability Office ("GAO"), "[c]yber-based intrusions and attacks on federal systems have become not only more numerous and diverse but also more damaging and disruptive."[31] This is illustrated by the 2015 data breach at OPM, which compromised the background investigation records of 21.5 million individuals.[32] More recently, a 16-year-old teenage boy was arrested in connection with hacks that exposed the information of more than 20,000 FBI employees and 9,000 Department of Homeland Security ("DHS") employees, as well as the personal email accounts of DHS Secretary Jeh Johnson and Central Intelligence Agency ("CIA") director John Brennan.[33]

The latest series of high-profile government data breaches indicates that federal agencies are incapable of adequately protecting sensitive information from improper disclosure. Data breaches are not an "if" but a "when." Indeed, GAO recently released a report on widespread cybersecurity weaknesses throughout the executive branch, aptly

---

https://www.washingtonpost.com/news/the- switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breaches/.

[30] OPM, *Cybersecurity Resource* Center, https://www.opm.gov/cybersecurity/cybersecurity-incidents/#WhatWeAreDoingToHelp.

[31] U.S. Gov't Accountability Office, *DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System* (Jan. 2016), http://www.gao.gov/assets/680/674829.pdf [hereinafter "GAO Cybersecurity Report"].

[32] GAO Cybersecurity Report at 8.

[33] Alexandra Burlacu, *Teen Arrested Over DHS and FBI Data Hack*, TECH TIMES (Feb. 13, 2016), http://www.techtimes.com/articles/133501/20160213/teen-arrested-over-dhs-and-fbi-data-hack.htm.

titled "Federal Agencies Need to Better Protect Sensitive Data."[34] According to the report, a majority of federal agencies, "have weaknesses with the design and implementation of information security controls . . . ."[35] The GAO report concluded that, due to widespread cybersecurity weaknesses, most federal agencies, "federal systems and information, as well as sensitive personal information about the public, will be at an increased risk of compromise from cyber-based attacks and other threats."[36]

b. Retention of a Massive Biometric Database Increases Privacy and Civil Liberties Risks Due to Bad Actors, Mistakes, and Mission Creep

The NGI database contains biometric data on millions of individuals, data the FBI plans to keep well beyond the time necessary for the purpose of its collection. The collection of biometrics itself by the FBI raises privacy and civil liberties risks. The retention of this data decades beyond that which is necessary intensifies these risks.

Large biometric databases like NGI have the potential to destroy the ability of an individual to be anonymous. Publicly participating in society as a relatively anonymous individual becomes increasingly impossible if every fingerprint left behind, image from a camera or CCTV, or recording of one's voice becomes an identifier; an identifier that can reveal the protests one participate in, the groups one associate with, or the things one spoke out about. NGI will increase the government's ability to do surveillance on individuals, including individuals who are not suspected of any wrongdoing.

Facial recognition in particular threatens privacy and civil liberties because it can so easily be done covertly, even remotely, and on a mass scale. Ubiquitous and near-

[34] U.S. Gov't Accountability Office, *Federal Agencies Need to Better Protect Sensitive Data* 4 (Nov. 17, 2015), http://www.gao.gov/assets/680/673678.pdf
[35] *Id*. at unpaginated "Highlights" section.
[36] *Id*. at 12.

effortless identification eliminates individuals' ability to control their identities and poses a special risk to the First Amendment rights of free association and free expression, particularly for those engaged in lawful protests.

A recent GAO report assessed the FBI's use of facial recognition and found that the agency failed to conduct a privacy audit to ensure that the use of facial recognition by the FBI was inline with the Fair Information Practices and consistent with FBI's stated policies and agreements.[37] The GAO also found that the FBI failed to test the accuracy of its facial recognition technology.[38] Furthermore, the report stated that the FBI did not update the public in a timely fashion regarding its use of facial recognition.[39] The FBI now wants to exempt itself from the Privacy Act and remove what little safeguards are in place to protect individuals' biometric data from privacy and civil liberties abuses.

IV. FBI's Broad Privacy Act Exemption Claims Remove Any Meaningful Privacy Safeguards for Vast Biometric Database

FBI claims numerous Privacy Act exemptions for NGI—exempting NGI from §§ 552a(c)(3)-(4); (d)(1)-(4); (e)(1)-(3); (e)(4)(G)-(I); (e)(5); and (e)(8)(f)-(g). The FBI's claimed exemptions exacerbate the privacy and civil liberties risks of the Bureau's massive biometric database.

For example, FBI exempts itself from § 552a(e)(1), which requires agencies to maintain only those records relevant to the agency's statutory mission. The agency exempts itself from § 552a(e)(4)(I), which requires agencies to disclose the categories of sources of records in the system. And the agency exempts itself from its Privacy Act

[37] GAO Face Recognition Report at 23-24.
[38] *Id.* at 26-27.
[39] *Id.* at 21.

duties under to § 552a(e)(4)(G) and (H) to allow individuals to access and correct information in its records system. In other words, the FBI claims the authority to collect any information it wants without disclosing where it came from or accounting for its accuracy or acknowledging its existence.

The FBI attempts to circumvent the intent of the Privacy Act by expanding a massive government database of detailed personal information that lacks accountability. The FBI's proposed exemptions from 5 U.S.C. § 552a(c)(3), (e)(8), and (g) only serve to increase the secrecy of the database and erode agency accountability. The FBI claims that accounting for disclosures, granting individuals access to their records, and implementing notification regulations may put entities on notice that they are being investigated, thereby hindering their investigative efforts.[40]

While EPIC recognizes the need to withhold notice during the period of the investigation, individuals should be able to know, after an investigation is completed or made public, the information stored about them in the system. Access to records of a completed investigation, with appropriate redactions to protect the identities of witnesses and informants, would provide individuals and entities with the right to address potential inaccuracies. And because the investigations have already been completed, FBI's law enforcement purposes would not be undermined and the FBI could still protect individual privacy rights.

The FBI also proposes to exempt NGI from requirements for maintain accurate, relevant, timely, and complete information. Such exemptions increase the privacy risks to individuals in the NGI database. These risks are exacerbated by the fact that over "18,000

[40] NGI NPRM at 27,289.

local, state, tribal, and federal law enforcement agencies across the country" have some form of access to the data maintained in NGI.[41] The FBI previously recognized the multitude of risks associated with NGI in the various Privacy Impact Assessments associated with the system. The FBI listed the requirements of the Privacy Act multiple times as a mitigating factor against the privacy risks associated with NGI.[42] Now the FBI proposes to take those safeguards away.

The Privacy Act is intended to guard the privacy interests of citizens and lawful permanent residents against government intrusion and to establish accountability for the government's collection and use of personal information. By asserting a multitude of exemptions that remove the safeguards of the Privacy Act, the FBI violates the central purpose of the Privacy Act and further removes NGI from public transparency. At the same time the FBI seeks to deny individuals access to the data collected about them, the Bureau proposes to expand access to the data across government agencies at every level.

U.S. District Judge Tanya Chutkan, in a Freedom of Information Act lawsuit against the FBI, clearly described the basis for public interest in NGI, stating "[t]here can be little dispute that the general public has a genuine tangible interest in a system

---

[41] FBI, *Next Generation Identification - Implementing the Future of Identification & Investigative Services*, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/biometric-center-of-excellence/files/ngi-one-pager-final.pdf.

[42] *See* FBI**,** *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) – Interstate Photo* System, § 2.3 (September 2015), https://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system; FBI, *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) –Palm Print and Latent Fingerprint Files*, § 5.4 (January 20, 2015), https://www.fbi.gov/foia/privacy-impact-assessments/next-generation-identification-palm-print-and-latent-fingerprint-files; FBI, *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) - Retention and Searching of Noncriminal Justice Fingerprint Submissions*, § 2.3 (February 20, 2015), https://www.fbi.gov/foia/privacy-impact-assessments/next-generation-identification-ngi-retention-and-searching-of-noncriminal-justice-fingerprint-submissions.

designed to store and manipulate significant quantities of its own biometric data, particularly given the great numbers of people from whom such data will be gathered."[43]

V. Conclusion and Recommendations

For the foregoing reasons, the FBI's proposed exemption of NGI is contrary to the core purpose of the federal Privacy Act. Accordingly, FBI must narrow the scope of its proposed Privacy Act exemptions and severely limit the data collected and the length of retention of that data.

Respectfully Submitted,

Marc Rotenberg
EPIC President and Executive Director

Jeramie D. Scott
EPIC National Security Counsel

Natasha Amlani
EPIC Law Clerk

Eva Gloster
EPIC Law Clerk

[43] *EPIC v. FBI*, 72 F. Supp. 3d 338, 346 (D.D.C. Nov. 5, 2014).