CENTER FOR DEMOCRACY & TECHNOLOGY

July 6, 2016

Privacy Analyst, Privacy and Civil Liberties Office
Department of Justice
National Place Building
1331 Pennsylvania Ave. NW, Suite 1000
Washington, DC 20530

VIA ELECTRONIC SUBMISSION

Re: Comments of the Center for Democracy and Technology on the Federal Bureau of Investigation's Proposed Rulemaking to Exempt the System from Provisions of the Privacy Act (CPCLO Order No. 003-2016) and the Modified System of Records Notice for the Next Generation Identification System (CPCLO Order No. 002-2016)

1. Introduction

The Center for Democracy and Technology ("CDT") respectfully submits these comments urging the Department of Justice ("DOJ") and the Federal Bureau of Investigation ("FBI") to reconsider the proposal in CPCLO Order No. 003-2016 to broadly exempt the Next Generation Identification ("NGI") biometric system[1] from key provisions of the Privacy Act of 1974.[2] CDT also offers comments on the modified system of records notice in CPCLO Order No. 002-2016.

CDT is a nonprofit public interest group that seeks to promote free expression, privacy, individual liberty, and technological innovation on the open, decentralized internet. CDT supports laws, corporate policies, and technical tools that protect the civil liberties of internet users. CDT represents the public's interest in an open internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

While the FBI may be able to articulate instances where criminal records in the NGI could properly be exempted under specific provisions of the Privacy Act, an exemption of the scope proposed—which would cover, for instance, records about individuals who have never encountered the criminal justice system in any form, let alone been convicted of a crime—is inappropriate and poses significant peril for privacy and civil liberties.

---

1 Justice/FBI-009.

2 Pub. L. No. 93-579, 88 Stat. 1896 (1974) (codified at 5 U.S.C. § 552a (2012)).

Currently, the NGI includes a number of different biometrics, including fingerprints, face recognition data, iris scans, and palm prints. These records may be collected not just during arrests, but also during any "criminal inquiry" or "lawful detention."[3] Additionally, the NGI contains entirely civil records, such as fingerprints and other biometrics of individuals in the military, individuals applying for immigration "or other governmental" benefits, individuals seeking permanent residency or citizenship, individuals who have applied for a security clearance, and individuals at all levels of government who have been fingerprinted as part of licensing or a background check for employment.[4]

In the NGI Privacy Impact Assessments ("PIAs") published in 2015,[5] the FBI announced that it would create a single identity file that would link criminal and civil fingerprint data, and would permit the searching of certain civil records in criminal contexts. In practice, we understand this to mean that if one applies for a security clearance or for a job even at a state or local level, for instance, fingerprints submitted as part of the application would be searched thousands of times a day by federal, state, local, tribal, territorial, and international law enforcement agencies for investigative leads.[6]

As described in the SORN, the NGI database represents a sea change in how the government collects, stores, retains, and disseminates biometric data in the pursuit of crime. The SORN erases the line between civil records, collected from individuals who have done nothing wrong and who have never interacted with law enforcement, and verifiable criminal biometrics.[7] Under the SORN, both can now be searched, cross-referenced, linked and then used to generate investigative leads or, if the civil record contains a ten-print fingerprint, used to positively identify suspects.

As discussed in greater detail below, we offer comments on a number of different issues with the NGI:

---

[3] Notice of a Modified Systems of Record Notice, 81 Fed. Reg. 27,284 (May 5, 2016) [hereinafter *SORN*].

[4] *Id.* at 27,284-85.

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

[6] *Noncriminal Justice Fingerprint PIA*, *supra* note 5, § 1 ("[O]nce civil fingerprints are retained in NGI, all incoming civil and criminal fingerprints will cascade against those fingerprints, and latent fingerprint contributors may choose to have their latent fingerprints cascade as well.").

[7] Granted, that line has been blurred in NGI's predecessor systems.

- The Privacy Act is an essential check against government misuse of personal data. Enacted in the wake of Watergate and revelations that elements of the intelligence community, military, and law enforcement had collected dossiers on individuals based on the exercise of their First Amendment rights, the law gives individuals the ability to access their records and correct mistakes. It also gives individuals the ability to take legal action against a government entity that, for instance, maintains dossiers based on First Amendment activity.[8] The proposed exemption would eliminate these protections.

- The FBI cannot rely on the general exemptions of 5 U.S.C. § 552a(j) (2012) for the civil records in NGI. By their terms, the general exemptions are only permissible for Central Intelligence Agency and law enforcement records.

- The multi-biometric NGI is a much more powerful and intrusive database than its fingerprint-based forebears.[9] Accordingly, the risks of false positives, which have been documented already in this context, are significant. This danger can be at least somewhat ameliorated by the provisions of the Privacy Act that permit individuals to access and correct inaccurate records, which would be exempted under the FBI's proposal (and would be unenforceable as the remedies section would also be exempt).

- Broadly, the existence of the NGI could chill the exercise of First Amendment rights. There are indications that the NGI database will include biometrics gathered in the field, including biometrics from individuals who are wrongly arrested, or who are subject to "lawful detention" but not arrested or charged. These elements of the system may be particularly burdensome for protesters and other individuals engaged in protected First Amendment activity.

- Finally, as is the case with "big data" in the non-law enforcement context, inherent systemic biases will creep into NGI if not guarded against through procedural protections like the Privacy Act. Disparities in the criminal justice system can only be amplified by NGI. Limiting any Privacy Act exemptions will mitigate this risk.

2. Importance of the Privacy Act

The Privacy Act grew out of two phenomena. The first was the Watergate scandal and revelations of politically motivated spying by law enforcement and the intelligence community. The second was the rapid growth in the mid-1970s of automated information collection,

---

[8] 5 U.S.C. § 552a(e)(7) (2012) (agencies may not maintain records "describing how any individual exercises rights guaranteed by the First Amendment" unless expressly authorized by statute or by the person about whom the records are held, or if the records are pertinent to and within the scope of an authorized law enforcement activity).

[9] Previous systems included limited biometric records beyond fingerprints, but they were not searcheable. *See SORN*, *supra* note 3, at 27,284. They also did not retain civil fingerprints, unlike NGI. Once processed, civil fingerprints were destroyed. *Noncriminal Justice Fingerprint PIA*, *supra* note 5, § 1.

retention, and dissemination by the government. As the House committee considering the bill noted:

> Accelerated data sharing of such personally identifiable information among increasing numbers of Federal agencies through sophisticated automated systems, coupled with the recent disclosures of serious abuses of governmental authority represented by the collection of personal dossiers, illegal wiretapping, surveillance of innocent citizens, misuse of income tax data, and similar types of abuses, have helped to create a growing distrust, or even fear of their Government in the minds of millions of Americans.[10]

Along with other measures designed to promote government transparency and check abuses, such as the earlier Freedom of Information Act, the Privacy Act embraces institutional checks and balances that guard civil liberties by increasing the opportunity for government waste or abuse to be revealed. The Privacy Act accomplishes this by providing three key protections: the right to access information held by the government about the requestor, the right to correct or delete inaccurate or outdated information, and the right to sue the government to enforce these rights.

The FBI proposes to broadly exempt the NGI from all three of these protections.[11] Particularly troubling is the FBI's claimed exemption for subsection (g), which sets out remedies and a statutory right of action for denial of access, refusal to correct a record, or failure to comply with any other Privacy Act provision or rule that has an adverse effect on an individual. In effect, this would exempt the NGI from *any* provision of the Privacy Act, even those that are not enumerated by the FBI in the NPRM.

For instance, the Privacy Act bars agencies from maintaining records describing how an individual exercises rights guaranteed by the First Amendment. Under the SORN, such records could be included in the NGI. Consider, for instance, law enforcement photos of an arrest at a protest. Based on the broad language of the SORN, and under even the current language of the

---

[10] *See, e.g.*, Staff of S. Comm. On Government Operations, 94th Cong., Legislative History of the Privacy Act of 1974, S. 3418 (Public Law 93-579) 295 (1996).

[11] Specifically, the FBI proposes to exempt NGI from 5 U.S.C. § 552a(c)(3) and (4) (covering the disclosure of personal records with other agencies); (d)(1), (2), and (3) (providing for access to one's record and the ability to request corrections); (e)(1), (2), and (3) (requiring the government to limit the collection of information to only that relevant and necessary to the reason for the collection and requiring notice to the individual of the authority under which the government is doing the collecting); (e)(4)(G), (H), and (I) (requiring the government to publish notices in the Federal Register informing individuals of the procedures whereby they can access and contest records held by the government about them); (e)(5) (ensuring fairness when records are used in making a determination about an individual); (e)(8) (providing for notice when records are disclosed under compulsory process); (f) (governing when an agency must publish rules under the Privacy Act); and (g) (setting out remedies, including a right of action and federal jurisdiction). Notice of Proposed Rulemaking, 81 Fed. Reg. 27,288 (May 5, 2016) [hereinafter *NPRM*].

relevant PIA, these arrest or detention photographs could include pictures of surrounding individuals who are simply attending the protest—clearly First Amendment protected activity.[12]

These images could then be searched by law enforcement and used to generate investigative leads. An individual would not be able to sue the government were those images maintained in the NGI in violation of this provision.

Similarly, 5 U.S.C. § 552a(e)(6) (2012)—also not one of the claimed exemptions—requires an agency to make "reasonable efforts" to assure the accuracy and completeness of records before dissemination outside the agency. Indeed, the FBI has pointed to this provision as an important check against any abuse of the system.[13] Were the FBI to share inaccurate or incomplete NGI records in violation of this provision, however, individuals would likewise not be able to sue.

Because it comingles criminal and civil records, and is used for both criminal and civil purposes, the NGI is precisely the type of database that drove passage of the Privacy Act in the wake of Watergate and revelations of illegal government spying. Inaccurate, incomplete, irrelevant, or outdated information in the database could lead to criminal scrutiny of entirely innocent individuals. It is imperative than any Privacy Act exemptions be, at a minimum, limited to sensitive criminal records.

3. Failure to Articulate a Sound Basis for the Assertion of Exemptions Under Either the General or Specific Exemptions of the Privacy Act

As explained in more detail in comments offered by the Center for Privacy and Technology at the Georgetown University Law Center, the FBI has not met its obligation under the Privacy Act to adequately explain why certain records are subject to either the general or specific exemptions under the Privacy Act.

---

[12] Granted, in the PIA, the FBI has said that "probe" photographs such as a picture of an arrestee at a protest that captures surrounding faces will not be retained and that civil images will not be searched for criminal investigative leads. Both of these limits, while clearly important, have been imposed at the discretion of the FBI and may be weakened or eliminated in the future. *Interstate Photo System PIA*, *supra* note 5, § 1. Further, non-mugshot photos will be retained and searched in two contexts: civil photographs that are linked by matching fingerprints to a criminal file and photographs in the Unsolved Photo File, which, by their nature, could include pictures of individuals at a protest if the submitter is investigating a felony crime against a person. *Id.* As for language in the SORN that would cover a protest photo, many could, but categories (G) and (K) of covered individuals broadly encompass biometrics obtained "as a result of a criminal inquiry, a lawful detention, an arrest, incarceration, or immigration or other civil law violation" and those collected "pursuant to the FBI's authority to identify and investigate federal crimes and threats to the national security." *SORN*, *supra* note 3, at 27,285. Nothing in the SORN limits the collection of facial images to the claimed offender or to mugshots, and nothing prevents the FBI from changing its stated policy and beginning to retain and search probe photos.

[13] *Id.* § 2.3.

The Privacy Act includes two sets of "exemptions," general and specific. General exemptions may only be claimed by the CIA, or, by law enforcement agencies *if* they can show that the records fall into one of three buckets: (1) information compiled to identify individual offenders that is limited to arrest data and information about the disposition of a matter; (2) information associated with an identifiable individual compiled for the purpose of a criminal investigation; or (3) reports identifiable to an individual compiled at any stage of the criminal justice process.[14]

Civil records would not fall into these categories based on a plain reading of the statute. Accordingly, the FBI's assertion of exemptions with regard to sections (c)(4), (e)(2) and (3), (e)(5), (e)(8), and, most importantly, the civil remedies section (g) is textually inappropriate with respect to civil records. With respect to the remedies section, and given that the NGI is predominantly a criminal investigative tool, it is crucially important that individuals be able to enforce their rights under the Privacy Act as applied to civil records held in NGI.

The FBI has also failed to properly articulate why information other than truly sensitive investigative material qualifies for the specific exemptions triggered by 5 U.S.C. § 552(k)(2) (2012) for "investigatory material compiled for law enforcement purposes."

First, much of the SORN (the systems of records notice released by the FBI in May that describes what is in the database) is impermissibly vague and allows for future changes to the types of records included in the system and the uses of those records. For instance, the SORN states that the NGI will include biometrics from individuals collected as a result of a "lawful detention . . . or other civil law violation," both of which encompass a broad array of pre-arrest encounters with law enforcement.[15]

The term "lawful detention" could include instances where biometrics have been collected during the course of a sobriety checkpoint or during a "stop-and-frisk" program where officers are directed to aggressively engage in temporary detentions. In both of these cases, biometrics could be included in the NGI even though the individuals detained are released without arrest or charge. Likewise, the phrase "other civil law violation" encompasses a vast universe of possible laws and regulations, many quite minor, at all levels of government.

Additionally, the NPRM claims an exemption from section (e)(5) because "it is impossible to determine in advance what information is accurate, relevant, timely and complete" and because over time "seemingly irrelevant or untimely information may acquire new significance when new details are brought to light."[16]

---

[14] 5 U.S.C. § 552a(j)(1)-(2) (2012).

[15] *SORN*, *supra* note 3, at 27,285.

[16] *NPRM*, *supra* note 11, at 27,289.

In these and other cases, the FBI has failed to meet its burden to articulate with specificity the records at issue and the reason for exempting them from the Privacy Act exemption that pertains to legitimate investigative records.[17]

Finally, as also noted by the Center for Privacy and Technology, the proposed exemption from 5 U.S.C. § 552a(c)(3) (2012) is improper. That section requires a record holder to disclose the "accounting" created when a record is shared with another agency or person. The FBI claims that this section would permit an individual to request the accounting in such a way that it could tip the individual off to investigative interest by the FBI.[18] This ignores the specific exceptions in § 552(b)(1), which does not require accounting in the case of internal agency sharing in the performance of the agency's duties, and § 552a(b)(7), which specifically exempts disclosures to other agencies for law enforcement purposes.

4. Danger and Consequences of False Positives

The primary danger in the NGI system is that it will generate false investigative leads that implicate innocent people in crime. This danger is particularly acute in the facial recognition context, where false positives can be high and the civil liberties consequences of a false match severe.

Indeed, the Government Accountability Office ("GAO") released a report in June critical of the FBI's facial recognition capabilities.[19] The report found that the FBI had conducted limited testing to evaluate the extent to which facial recognition searches in the NGI database turned up matches to persons in the database (the detection rate), but did not test the false positive rate (when the system erroneously matches a person not in the database to an image in the database).[20] The FBI also failed to test either the detection rate or the false positive rate when returning searches of fewer than 50 candidates (searches that return 2 to 50 candidates are permissible by NGI users).[21]

Finally, the report noted that the FBI initially estimated a *20 percent* false positive rate, but then felt that testing the rate was unnecessary given that the system was producing 50 possible

---

[17] *See Doe v. FBI*, 936 F.2d 1346, 1352-53 (D.C. Cir. 1991) (noting that the claimed exemption for the FBI's Central Records System ("CRS") only applies to records that qualify as law enforcement records and that records derived from the FBI's "merely engaging in a general monitoring of private individuals' activities" do not qualify for the exemption).

[18] *NPRM*, *supra* note 11, at 27,289.

[19] U.S. Gov't Accountability Office, GAO-16-267, Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy (2016) [hereinafter *GAO Report*].

[20] *Id.* at 26-27.

[21] *Id.* at 26.

matches at an 80 percent detection rate.[22] The GAO, however, noted that the false positive rate is both testable and an important metric, especially if, as is expected, the detection rate would drop as the number of possible matches requested goes down.[23]

The report concluded that "[g]iven that the accuracy of a system can have a significant impact on individual privacy and civil liberties as well as law enforcement workload, it is *essential* that both the detection rate and the false positive rate for all allowable candidate list sizes are assessed prior to the deployment of the system."[24]

This is particularly problematic in that the accuracy of the facial recognition technology at issue—which seeks to match an individual face to an individual face—can be influenced by the quality of the images used to do the matching. Accuracy increases as the quality of the photos increases, and as things like lighting, the relative position of the face in each photo (e.g., head-on versus a side view), and the age of the subject in each photograph match more closely. By contrast, accuracy suffers when the "probe" photo is of lesser quality, or depicts the subject in a way different from the record in the database.

As noted, false positives in the law enforcement context raise unique civil liberties and privacy concerns as each false match can result in law enforcement scrutiny of an innocent individual. At the very least, the FBI should follow the GAO's recommendations and accurately test both the detection rate and the false positive rate for all allowable candidate list sizes.[25]

5. Implications for the First Amendment

The NGI raises First Amendment concerns to the extent that it includes biometrics from individuals who are merely exercising their First Amendment rights. The NGI enhancements over its predecessor, the Integrated Automated Fingerprint Identification System ("IAFIS"),

---

22 *Id.*

23 *Id.* at 26-27.

24 *Id*. at 27 (emphasis added).

25 In its response to the GAO, the DOJ disagreed with this recommendation, arguing that, because the query returns a candidate list and does not technically provide positive identification, it need not test either the detection rate or the false positive rate at every allowable candidate list size. *Id.*, app. IV at 8 ("[D]ue to the fact that no positive identifications are made based on NGI-IPS searches, there are also no false positive identifications."). This does not address the GAO's point. First, irrespective of whether a candidate list can produce positive identification, the detection rate at different candidate list sizes remains important. As the FBI itself noted, as the candidate list size goes down, so does the detection rate. *Id.* at 38. Second, even though facial recognition cannot produce a positive identification, it *can* produce investigative leads. Further, given that candidate lists are ranked, not all candidates are "equal" in the eyes of the submitter. Higher ranked candidates may receive more scrutiny than lower ranked candidates, and inaccuracy may still implicate innocent people in criminal investigations. Third, there absolutely can be false positives in a ranked candidate list. That is, the system may return a "hit" when in fact the person in the probe photo does not exist at all in the NGI system.

heighten this concern in several ways, which flow from the possibility that records of individuals that have not been arrested, or have been improperly arrested, will be included in the NGI and searched for criminal leads.

First, the DOJ currently states that the searchable photo database, the Interstate Photo System, only includes "criminal mugshots obtained pursuant to arrest and associated with ten-print fingerprints . . . in accordance with the existing IAFIS SORN" and that "[c]riminal photos that do not meet a probable cause standard or that are not positively associated with criminal fingerprints are not available for searching."[26]

The IAFIS SORN, however, will not be the governing document going forward. The NGI SORN, which will apply, is unquestionably much more expansive than IAFIS. Among the categories of criminal photographic records covered by the NGI SORN are those that have been obtained as a "result of a criminal inquiry, a lawful detention, an arrest, incarceration, or immigration or other civil law violation" and those that have been "retrieved from locations, property, or persons associated with criminal or national security investigations."[27] Both of these categories, by their terms, go far beyond a criminal mugshot.[28]

Expanding the universe of searchable photographs beyond the mugshot poses special challenges for the First Amendment. The FBI's proposal could sweep in new categories of biometrics gathered in the field—including facial images obtained through CCTV, webcam, or drone footage. Further, when an FBI investigation turns to social media, the universe of photographs that could be included and searched via NGI grows dramatically. For instance, an NGI that includes social media photographs could be searched to identify attendees at political rallies or prayer services, screen visiting scholars for undisclosed social media profiles, or identify a journalist's confidential government source.

Even were the NGI-IPS database limited to criminal mugshots,[29] it could have serious First Amendment implications. Currently, in addition to racial and ethnic minorities, groups that are at risk of being inappropriately included in the database include individuals improperly arrested

---

[26] *Id.*, app. IV at 4.

[27] *SORN*, *supra* note 3, at 27,285.

[28] As discussed in note 12, *infra*, the Interstate Photo System PIA states that probe photos are not retained and civil photos are not searched against probe photos. Nevertheless, images of individuals merely exercising their First Amendment rights may currently enter the system in two ways, even were the current PIA to stand following the issuance of the broad NGI SORN. First, probe photos may, and likely will, contain images of individuals surrounding the subject, and these may be searched against the IPS repository. A false match could result in investigative interest. Second, images in the Unsolved Photo File may include the proverbial "protest photo."

[29] The SORN, NPRM and Interstate Photo System PIA also make no provision for the deletion of mugshots obtained when the charges are dropped, the individual is acquitted, or the charges are ordered expunged.

and photographed while engaging in peaceful protest,[30] recording the police,[31] and holding officials accountable by means of investigative reporting and records requests.[32] Without any protections for biometrics obtained in improper or mass arrests, activists and citizen journalists will be chilled from engaging in protected activity for fear that their pictures, iris scans, palm prints, and other biometrics will one day turn up a match in the NGI.

Consequently, this is an area where Privacy Act remedies are particularly important, and the FBI's claimed exemption from 5 U.S.C. § 552a(g) (2012) particularly troubling.

6. Amplifying Disparities in the Criminal Justice System

The NGI system is different from its predecessors. Unlike IAFIS, it seeks to link criminal and civil fingerprints, photographs, palm prints, iris scans, and many other biometrics (including those the FBI has not considered yet for inclusion) into a single record.[33] Any biases in the underlying data—along racial, ethnic, religious, socio-economic, or other lines—will be amplified by the system.

For instance, the SORN makes clear that individuals fingerprinted as part of a "lawful detention,"[34] which includes a "Terry" stop, are covered by the system.[35] Due process concerns aside (such individuals are stopped on the basis of something less than probable cause and may never be arrested, let alone charged with a crime), biometrics gleaned from Terry stops are likely to be racially skewed. For instance, a 2009 review of New York City's "stop-and-frisk"

---

[30] Taylor Wofford, *Police Arrest Dozens of Black Lives Matter Protesters, Body Slam Man in Ferguson*, Newsweek (Aug. 10, 2015), http://www.newsweek.com/ferguson-police-black-lives-matter-protests-361765; *51 Arrested in Protests After Black Man Shot by Minneapolis Police*, USA Today (Nov. 17, 2015), http://www.usatoday.com/story/news/nation-now/2015/11/16/minneapolis-police-shooting/75859132/.

[31] John Marzulli, *NYPD Accused of Arresting Man for Recording Video of Cops Cuffing Woman*, N.Y. Daily News (June 16, 2016), http://www.nydailynews.com/new-york/nypd-accused-arresting-man-recording-video-cops-article-1.2675620; Frank Eltman, *Citizens Filming Police Often Find Themselves Arrested*, Assoc. Press (Aug. 30, 2015), *available at* http://www.abqjournal.com/636460/citizens-filming-police-often-find-themselves-arrested.html.

[32] Rhonda Cook, *North Georgia Newspaper Publisher Jailed Over Open Records Request*, Atlanta Journal-Constitution (July 2, 2016), http://www.myajc.com/news/news/local/newspaper-publisher-indicted-jailed-over-public-re/nrqgq/.

[33] As noted, current DOJ policy is to exclude civil photographs from the searchable NGI-IPS database, but that policy could change in the future, and the SORN clearly states that civil photographs could be included in the database. In cases where fingerprints submitted along with a civil photo match fingerprints submitted as part of the criminal repository, the two photos are linked, and those civil photos become searchable for criminal leads. *Interstate Photo System PIA*, *supra* note 5, § 1.

[34] *SORN*, *supra* note 3, at 27,285.

[35] *See Terry v. Ohio*, 392 U.S. 1 (1968).

program, which was based on deliberately aggressive Terry stops, found that 80 percent of those detained were black and Latino, and only 10 percent of those stopped were white.[36]

And, indeed, there are indications that the NGI will include biometric data taken in the field. For instance, in March, a company called InCadence announced the award of a prime contract to provide the FBI with a mobile biometric solution using smart phones, which will be able to take fingerprints, facial photographs, and contextual information.[37] Accordingly, were NGI expanded to include photographs and fingerprints taken in the field during high-arrest programs like stop-and-frisk, racially skewed data could well end up in NGI, which heightens the risk that it will entrench current disparities in the criminal justice system.

Biometric data collected even during proper arrests can amplify disparities. A USA Today analysis of arrest records found that at least 1581 police departments nationwide arrested blacks at rates three times that of white suspects, with at least 70 departments from Connecticut to California arresting blacks at rates ten times higher than their white counterparts.[38]

These disparities persist for similarly situated defendants. For instance, following legalization of marijuana in Colorado, arrest rates for marijuana cultivation dropped dramatically for whites but ticked up slightly for black defendants.[39]

The inclusion of biometrics collected from immigration enforcement actions, too, serves to perpetuate racial disparities in the NGI database. The very decision to use such records disproportionately impacts minorities; as a 2009 DHS report showed, the top ten countries of origin for undocumented immigrants were all in Latin America or in Asia.[40]

Immigration law enforcement, as well, has long been plagued by accusations of racial profiling. For instance, a 2011 analysis of a key Obama administration deportation program found that Latinos made up 93% of deportees, though they constitute only 77% of the undocumented

---

[36] Ctr. for Constitutional Rights, *Racial Disparity in NYPD Stops-and-Frisks, Preliminary Report* (2009), *available at* ccrjustice.org/sites/default/files/assets/Report-CCR-NYPD-Stop-and-Frisk_3.pdf.

[37] Press Release, InCadence, InCadence Strategic Solutions Wins Mobile Biometrics Prime Contract with the FBI (Mar. 21, 2016), *available at* https://incadencecorp.com/2016/03/20/incadence-fbi-contract/.

[38] Brad Heath, *Racial gap in U.S. arrest rates: 'Staggering disparity,'* USA Today (Apr. 19 2014), *available at* www.usatoday.com/story/news/nation/2014/11/18/ferguson-black-arrest-rates/19043207/.

[39] Jon Gettman, *Marijuana Arrests in Colorado After the Passage of Amendment 64*, Drug Policy Alliance (2015), *available at* https://www.drugpolicy.org/sites/default/files/Colorado_Marijuana_Arrests_After_Amendment_64.pdf.

[40] Michael Hoefer et al., *Estimates of the Unauthorized Immigrant Population Residing in the United States: January 2009*, Department of Homeland Security, Office of Immigration Statistics (2010), *available at* https://www.dhs.gov/xlibrary/assets/statistics/publications/ois_ill_pe_2009.pdf.

immigrant population. The report also found that the program resulted in the arrest of thousands of U.S. citizens.[41] Because U.S. Immigration and Customs Enforcement has used mobile fingerprinting units to take biometric measures from people it both detains without arresting and ultimately arrests,[42] the inclusion of immigration offenses in NGI could allow large numbers of inappropriate records into the database.

The data show, then, that the sources of biometrics that feed into NGI are more likely to include minorities than their share of the population, or even their share of those who commit crimes. Accordingly, because the data that feeds into the database contains racial disparities, its use to generate investigative leads or positively identify suspects will perpetuate those existing disparities. This likewise counsels in favor of limiting any Privacy Act exemptions to truly sensitive investigative material.

7. Conclusion and Recommendations

The NGI is primarily a crime-fighting tool, and an extraordinarily powerful one. Its use and misuse can lead directly to invasions of privacy or deprivations of liberty. While there may be instances where records in the NGI system could appropriately be exempted from certain Privacy Act provisions, the blanket exemptions proposed in the NPRM are inappropriate, and are doubly so given the breadth and vagueness of the SORN.

Consequently, the accountability facilitated by the Privacy Act is an essential protection here. Individuals whose records are included—especially those who are simply seeking a job or applying for government benefits—should be able to access and correct their records, and must be given a legal mechanism to enforce those rights.

This is all the more important given the dramatic shift the FBI's proposal represents in how biometric information is collected and used to detect, investigate, and prosecute crime. The FBI's proposal would effectively eliminate the line between civil and criminal biometric records. Under the terms of the systems of records notice, the FBI would be able to collect, retain, link, search, and disseminate both civil and criminal biometrics. Practically speaking, the FBI would be able to use records of individuals who have done nothing wrong to generate leads and identify suspects. That is nothing less than a sea change in the relationship between law enforcement and biometric data.

Accordingly, we urge the DOJ and FBI to: (1) maintain policies that limit searches of civil records for criminal purposes; (2) issue a new proposed rule with more tailored proposed exemptions from the Privacy Act; (3) issue a new SORN that details precisely which records will be included in the NGI and how they will be used, retained, and shared; and (4) adopt the

---

[41] Aarti Kohli et al., *Secure Communities by the Numbers: An Analysis of Demographics and Due Process*, Chief Justice Earl Warren Institute on Law and Social Policy 2 (2011).

[42] Zoë Carpenter, *How the Government Created 'Stop-and-Frisk for Latinos'*, The Nation (Sept. 22 2014), *available at* https://www.thenation.com/article/how-government-created-stop-and-frisk-latinos/.

GAO's recommendations with respect to facial recognition, including testing both the detection and false positive rate for all allowable candidate list sizes.

A massive biometric database that is used to identify individuals and generate investigative leads is a significant threat to civil liberties and privacy, and is precisely the type of threat that the Privacy Act was meant to guard against. It is essential that it contain appropriate checks and balances against abuse, which will both limit its impact on civil liberties and provide greater accuracy for law enforcement.

Please do not hesitate to contact Gabe Rottman, deputy director of the Freedom, Security and Technology Project at CDT, with any questions. He can be reached at grottman@cdt.org.

Sincerely,

Gabe Rottman
Deputy Director, Freedom, Security and Technology Project
Center for Democracy and Technology