

THE RUTHERFORD INSTITUTE

Post Office Box 7482
Charlottesville, Virginia 22906-7482

JOHN W. WHITEHEAD
Founder and President

TELEPHONE 434 / 978 - 3888
FACSIMILE 434/ 978 – 1789
www.rutherford.org

June 2, 2016

VIA ELECTRONIC SUBMISSION **ProposedRegulations@usdoj.gov**

Ms. Erika Brown Lee
U.S. Department of Justice
Privacy & Civil Liberties Office
Attn: Privacy Analyst
1331 Pennsylvania Ave. NW, Suite 1000
Washington, DC 20530-0001

Re: Privacy Act of 1974; Systems of Records
[CPCLO Order Nos. 002-2016, 003-2016]

Dear Ms. Brown Lee:

The following is The Rutherford Institute's analysis and comment on the Department of Justice's ("DOJ") proposed rule "Privacy Act of 1974; Implementation," 81 FR 27288-01.¹

The Rutherford Institute has a particular interest in preserving privacy safeguards established by Congress and has continuously sought to protect the effectiveness of the Privacy Act and similar legislative provisions.² It is in that capacity that we wish to (1) address the overly expansive scope of the individuals included in the Next Generation

¹ The Rutherford Institute is a national, non-profit civil liberties organization that specializes in legal matters associated with constitutional rights.

² See generally J. Kirk Wiebe, *NSA: The False Balance Between Security and Privacy*, THE RUTHERFORD INSTITUTE (Jan. 21, 2014), https://www.rutherford.org/publications_resources/oldspeak/nsa_the_false_balance_between_security_and_privacy (rejecting the notion that effective security measures have to come at the expense of citizens' right to privacy); Letter from the Privacy Coalition to Representative Bennie G. Thompson, U.S. House of Representatives (Oct. 23, 2009), https://www.privacycoalition.org/DHS_CPO_Priv_Coal_Letter.pdf (letter to Congress in which The Rutherford Institute joined a coalition of twenty other concerned organizations to investigate potential failure by the Department of Homeland Security in protecting the privacy of American citizens).

Information Database (“NGI System” or “NGI”), (2) express our opposition to the near-limitless power and control that would be granted the DOJ over information collected on law-abiding individuals, and (3) urge the DOJ to significantly narrow the Privacy Act exemptions requested for the database.

Background on the Privacy Act and the Next Generation Identification System

The proposed rule relates to the federal Privacy Act of 1974, 5 U.S.C. § 552a (the “Privacy Act”). The Privacy Act serves as an important safeguard to individual privacy by preventing misuse of Federal Records and allowing individuals to access and amend the records held by federal agencies when such information directly concerns them.

The Privacy Act was initially enacted in 1974 in order to serve as a balancing tool between the government’s need to maintain information about individuals with the rights of individuals to be protected against “unwarranted invasions of their privacy stemming from federal agencies’ collection, maintenance, use, and disclosure of personal information about them.”³ Although some commentators have criticized the effectiveness of the Privacy Act,⁴ civil liberties organizations have typically spoken in strong support of its provisions,⁵ and some have even encouraged the strengthening and modernization of the Act in order to make it more compatible with new concerns associated with the rapid rise of technological advances.⁶

The Next Generation Identification System is described by the FBI and DOJ as a system that utilizes several of the most technologically advanced surveillance mechanisms that are currently available.⁷ NGI also collects and retains an enormous amount of biometric information on millions of individuals.

³ DEP’T OF JUSTICE, PRIVACY ACT OF 1974 (2010), <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1279>.

⁴ *1974 Privacy Act Too Porous to Protect Today’s Citizens*, USA TODAY, Sept. 29, 2003, http://usatoday30.usatoday.com/news/opinion/editorials/2003-09-29-our-view_x.htm (citing various loopholes within the Privacy Act that weaken its general effectiveness).

⁵ Electronic Privacy Info. Center, Comments of the Electronic Privacy Information Center to the Department of Homeland Security: 038 Insider Threat Program System of Records (2016), <https://epic.org/apa/comments/EPIC-DHS-Inisder-Threat-Comments.pdf> (providing comments to a proposed rule filed by the Department of Homeland Security and arguing that the agency’s requested exemptions fell beyond the appropriate scope of the Privacy Act of 1974). See also G. Wayne Miller, *Is Privacy Dying? ‘Technology is Pervasive and Invasive’*, THE RUTHERFORD INSTITUTE (July 29, 2013), https://www.rutherford.org/publications_resources/tri_in_the_news/is_privacy_dying_technology_is_pervasive_and_invasive.

⁶ Gerry Smith, *ACLU: Privacy Act is ‘Outdated,’ Contains ‘Major Loopholes’*, THE HUFFINGTON POST, July 31, 2012, http://www.huffingtonpost.com/2012/07/31/aclu-privacy-act_n_1724764.html (describing testimony given by the ACLU’s legislative counsel at a Senate hearing concerning the Privacy Act of 1974 and its need for revision).

⁷ FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi (last visited May 30, 2016).

Although the FBI and DOJ have described the NGI System as essential to effective law enforcement, a large portion of the information contained in the database relates to civil and administrative matters rather than biometrics collected in connection with criminal activity.⁸

Potential Threats Arising from NGI Exemption from the Privacy Act of 1974

If the proposed rules are granted, the exemptions would limit the applicability of the Privacy Act in several significant and potentially harmful ways.

The NGI database includes records and biometric information on millions of people who have never committed or even been accused of a crime

First, although it is true that the NGI System includes information on criminals collected from state, local, and federal law enforcement agencies, the database also includes records and biometric information on millions of people who have never committed or even been accused of a crime. Nevertheless, because of the broad language contained in the proposed rule, a countless number of individuals would likely be denied access to their records despite the fact that there would not be any justifiable reason for the FBI to prevent them from accessing or amending such information. Although we are reasonably sympathetic to the FBI's interest in effective policing, we do not believe that achieving such a goal should come at the expense of citizens' privacy. Based on the categories of individuals who are included in the NGI System, it is unclear that the exemptions would provide any additional benefit to the FBI and DOJ other than the unrestrained ability to observe innocent persons. Such power appears to be completely at odds with the stated intentions of the Privacy Act.

It is unknown how often the facial recognition system produces false matches, or whether information has been improperly catalogued

Moreover, the fact that the NGI System receives information from state and local law enforcement agencies raises another set of potential concerns. In particular, in *Shadd v. United States*, the United States District Court for the Western District of Pennsylvania suggested that, although "the FBI cannot avoid all responsibility for the accuracy of the information in its criminal files," the FBI is also not required to ensure that all of the records received from state and local agencies are wholly correct.⁹ Additionally, because the technology included in the database is relatively new and limited information about

⁸ Notably, individuals who are required to be fingerprinted for employment, governmental benefits, routine background checks, and immigration are all included in the NGI System.

⁹ 389 F. Supp. 721 (W.D.P.A. 1975).

its accuracy has been released to the public, we are concerned that the NGI System may yield unacceptable error rates.¹⁰

It is unknown how often the facial recognition system produces false matches, or whether information has been improperly catalogued. As such, records held by the agency may contain errors whose correction would be necessary to promote the interests of justice. The ability of individuals to access and amend records held on them by the FBI seems like an important—if not essential—method of ensuring the careful and accurate maintenance of records. At the very least, it would appear that allowing possibly inaccurate records to remain unchecked within the system would result in the compilation of distracting and erroneous information. It seems probable that such an outcome would hinder rather than enhance the FBI’s ability to effectively carry out its law enforcement duties.

The proposed rule could leave citizens without any possible means of recourse should their privacy rights be violated

Finally, the proposed rule would exempt the FBI from 5 U.S.C. § 552a(g), which would theoretically prevent individuals from enforcing any Privacy Act violation or obtaining civil remedies for agency misconduct. Exemption from § 552a(g) would allow the FBI to escape liability even if the agency violates portions of the Privacy Act from which it is not explicitly exempt. In practice, this would apparently leave citizens without any possible means of recourse should their privacy rights be violated.

Based on the holding in *Shearson v. U.S. Dep’t of Homeland Security*,¹¹ we believe that such an exemption is unauthorized by the Privacy Act. In its discussion on the scope of § 552a(j), the court in *Shearson* stated that an agency cannot escape liability for violating “non-exemptible Privacy Act obligations simply by exempting itself from the Act’s civil-remedy provisions; rather, an agency may exempt a system of records from the civil-remedies provision only to the extent that the underlying substantive duty is exemptible under § 552a(j).”¹² In the presently proposed rule, therefore, it appears that the DOJ is attempting to over-extend the applicability of § 552a(j) by creating a blanket exemption to the FBI’s conduct.

Further, the court also held that “[u]nder the Act, agencies seeking to promulgate exemptions under § 552a(j) must publish the justification for doing so.”¹³ Notably, the notice published by the Department of Justice fails to articulate a single reason why the

¹⁰ Brendan F. Klare et al., *Face Recognition Performance: Role of Demographic Information*, 7 IEEE Transactions on Info. Forensics & Security 6, 1789 (2012) (finding that facial recognition systems tend to be less accurate when matching subjects that are young, black, and/or female).

¹¹ 638 F.3d 498 (6th Cir. 2011).

¹² *Id.* at 503 (emphasis in original).

¹³ *Id.* at 504.

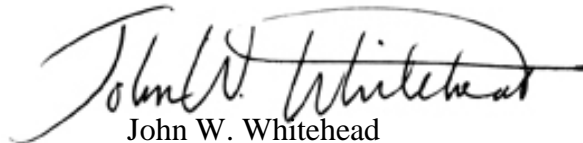
Ms. Erika Brown Lee
U.S. Department of Justice
June 2, 2016
Page 5

FBI should be exempted from the contents of § 552a(g). Thus, as the proposed rule presently stands, we do not believe that the DOJ's efforts at exempting the FBI from the Privacy Act's subsection on civil remedies adequately satisfy the procedural requirements.

The proposed rule is extraordinarily broad and would give the DOJ near-limitless power and control over information collected on law-abiding individuals.

Believing that the concerns outlined herein regarding the sensitive nature of the information contained in the NGI System, as well as the potential harm that could be caused to innocent people are significant enough to warrant greater oversight, The Rutherford Institute urges the Justice Department to reevaluate the contents of the proposal and to limit its scope to only that which is truly necessary for effective criminal law enforcement.

Sincerely yours,

A handwritten signature in black ink that reads "John W. Whitehead". The signature is written in a cursive style with a long horizontal flourish extending to the right.

John W. Whitehead
President

The Rutherford Institute