epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

DEPARTMENT OF JUSTICE

Privacy Act of 1974; Implementation

84 FR 49073

October 18, 2019

By notice published September 18, 2019, the Department of Justice's Federal Bureau of Investigation ("FBI") gave notice of a proposed rulemaking to change and expand their exemptions as well as provide the reasoning behind the exemptions for the National Crime Information Center ("NCIC").[1]

EPIC submits these comments to the FBI to urge the agency to: (1) comply with the Privacy Act; and (2) withdraw the proposed exemptions to Privacy Act protections.

EPIC is a public interest research center in Washington, D.C. EPIC that 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. EPIC has litigated cases against the Department of Justice to compel production of documents regarding "evidence-based risk assessment tools"[2] and the Department of

[1] Dep't of Justice, Federal Bureau of Investigation, *Privacy Act of 1974; Implementation*, 84 Fed.Reg. 49073 (September 18, 2019), https://www.federalregister.gov/documents/2019/09/18/2019-19448/privacy-act-of-1974-implementation.
[2] EPIC, *EPIC v. DOJ (Criminal Justice Algorithms)* https://epic.org/foia/doj/criminal-justice-algorithms/.

Homeland Security to compel production of documents about a program to "assess" the probability that an individual commits a crime.[3]

EPIC has long urged accuracy for the data held in the National Crime Information Center ("NCIC"). In 2003, EPIC organized a coalition of nearly 90 organizations to urge the Office of Management and Budget (OMB) to exercise the agency's oversight responsibilities and reestablish the accuracy requirements for NCIC.[4] After a leadership change at OMB, EPIC reiterated its demand that OMB address the FBI's overbroad exemption of the NCIC from Privacy Act requirements.[5] EPIC also submitted an amicus brief to the Supreme Court in *Herring v. US,* concerning the accuracy of records in police databases*,* urging the court to exclude evidence stemming from inaccuracies in NCIC.[6] EPIC also warned the Supreme Court in *Kansas v. Glover*[7] that mistakes in databases containing results from Automated License Plate Readers would like to unjustified car stops.

I. The FBI's Databases Consist of Massive Amounts of Highly Sensitive and Protected Information

The NCIC enables the transfer of detailed personal data between the FBI, federal, state, local and tribal criminal justice offices."[8] NCIC consists of 21 different files of information – organized in property files and person files. The property files consist of "records of stolen articles, boats, guns, license plates, parts, securities, and vehicles."[9] The persons files are: "Supervised Release; National

[3] *See Id.* and EPIC, *EPIC v. DHS (FAST Program)* https://epic.org/foia/dhs/fast/.
[4] EPIC, *Require Accuracy for NCIC*, https://epic.org/privacy/ncic/ (2003).
[5] EPIC Letter to OMB Director Joshua B. Bolten Re: NCIC Accuracy Concerns (February 20, 2004) https://www.epic.org/privacy/ncic/NCIC_letter.pdf.
[6] EPIC Amicus Brief, *Herring v. US*, 555 U.S. 135 (2009) https://epic.org/privacy/herring/07-513tsac_epic.pdf.
[7] EPIC Amicus Brief, *Kansas v. Glover*, 139 S. Ct. 1445 (2019) https://epic.org/amicus/fourth-amendment/glover/EPIC-Amicus-Kansas-v-Glover.pdf.
[8] FBI, *National Crime Information Center* (last visited October 1, 2019) https://www.fbi.gov/services/cjis/ncic.
[9] *Id.*

Sex National Sex Offender Registry; Foreign Fugitive; Immigration Violator; Missing Person; Protection Order; Unidentified Person; Protective Interest; Gang; Known or Appropriately Suspected Terrorist; Wanted Person; Identity Theft; Violent Person; and National Instant Criminal Background Check System (NICS) Denied Transaction."[10]

The system also contains images associated with many of these records and The Interstate Identification Index, which holds criminal history record information.[11] NCIC allows law enforcement officers (or other authorized non-law enforcement agent) to input information from their jurisdictions and access all of the other data included.

From its creation, the accuracy and use of NCIC records has raised concern. In 2002, over 3,000 individuals from 47 states and the District of Columbia signed on to a petition supporting stronger accuracy and misuse prevention requirements for NCIC.[12] There are numerous examples of misuse of NCIC records by law enforcement. An Associated Press report in 2016 found, "Police officers across the country misuse confidential law enforcement databases to get information on romantic partners, business associates, neighbors, journalists and others for reasons that have nothing to do with daily police work."[13] Furthermore, there have been well documented accuracy errors and auditing inadequacies.[14] The Supreme Court recognized this in Justice Ginsburg's dissent in *Herring v. United* States, stating that databases including NCIC have "dramatically expanded" in both "breadth and influence."[15] Meanwhile, the justice acknowledges government reports describing "flaws in NCIC databases, terrorist watchlist databases, and databases associated with the Federal

[10] *Id*.
[11] *Id*.
[12] EPIC, *Require Accuracy for NCIC*, https://epic.org/privacy/ncic/ (2003).
[13] *Police sometimes misuse confidential work databases for personal gain: AP*, CBS news, Sept. 30, 2016, https://www.cbsnews.com/news/police-sometimes-misuse-confidential-work-databases-for-personal-gain-ap/.
[14] EPIC Amicus, Brief, *Herring v. US*, 555 U.S. 135 (2009) https://epic.org/privacy/herring/07-513tsac_epic.pdf.
[15] *Herring v. United States*, 555 U.S. 135 at 155 (2009) (Ginsburg, J., dissenting).

Government's employment eligibility verification system" and explains that "inaccuracies in expansive, interconnected collections of electronic information raise grave concerns for individual liberty."[16]

A September 10 notice of modification of system of records proposes an expansion of NCIC, with new categories of records and individuals in the Supervised Release and Violent Person Files.[17] The System of Records Notice does not articulate the specific data points in the Supervised Release File; EPIC has submitted a Freedom of Information Act ("FOIA") request to discover if the results of pre-trial risk assessment tools are included in the Supervised Release File. The inclusion of this data would add another data point to NCIC rife with consistency, accuracy, and fairness concerns.[18]

II. Individuals Should be Able to Access their Personal Record Maintained in the NCIC

The FBI seeks to exempt the NCIC database from the following record-keeping obligations in the Privacy Act: (c)(3)-(4); (d); (e)(1)-(3), (4)(G)(H) and (I), (5), and (8); (f) and (g).[19] This proposal should be withdrawn.

The Privacy Act was enacted to ensure individuals know about information gathered by "Federal agencies, state and local governments, or any private organizations," and give an opportunity to inspect and dispute the records kept about them.[20] However, the FBI seeks to exempt

---

[16] *Id.*
[17] Dep't of Justice, Federal Bureau of Investigation, *Privacy Act of 1974; System of* Records, 84 Fed.Reg. 47533 (September 10, 2019), https://www.federalregister.gov/documents/2019/09/10/2019-19449/privacy-act-of-1974-system-of-records#print at 47533.
[18] *See e.g.* EPIC, Algorithms in the Criminal Justice System: Pre-Trial Risk Assessment Tools https://epic.org/algorithmic-transparency/crim-justice/; Melissa Hamilton, *The Biased Algorithm: Evidence of Disparate Impact on Hispanics*, 56 AM. CRIM L. REV. 1553 (2019) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3251763; Megan T. Stevenson, Christopher Slobogin, *Algorithmic Risk Assessments and the Double-Edged Sword of Youth*, Washington University Law Review, Vol. 96, 2018; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3225350; Julia Angwin, Jeff Larson, Surya Mattu, and Lauren Kirchner, *Machine Bias*, ProPublica (May 23, 2016) https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.w.
[19] *Supra* note 1 at 49074.
[20] Legislative History, Privacy Act of 1974 at pp.6-8 http://www.loc.gov/rr/frd/Military_Law/pdf/LH_privacy_act-1974.pdf.

the agency from the requirements of the Privacy Act that allow the agency to only maintain records relevant to the agency's mission;[21] to allow individuals to view the data about them in the FBI's records as well as correct and appeal incorrect data points;[22] and to maintain record with "such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record."[23]

All of these proposals should be withdrawn. The over collection and maintenance of information that is unverified and unaccountable with no system for redress leaves personal data at a risk.

The exemptions sought for §552(e)(1)-(3),(4)(g)-(i) concern the FBI's present requirements to maintain records only to an extent that it is relevant and necessary to accomplish a purpose of the

---

> "Under the provisions of the bill, information may be gathered by Federal agencies, State and local governments, or any private organizations only to accomplish the proper purpose of those agencies and organizations.
>
> In gathering information, the individual must be the source of that information to the greatest extent possible; however, no individual may be forced to disclose any information not required by law, and he is to be informed of his right not to disclose. The individual is to be notified of the existence of any information being maintained on him and the uses to which that information IS being put. No public or private organization may collect information on an individual's political or religious beliefs or affiliations unless specified by law. A description of all information systems must be reported to the Federal Privacy Board on an annual basis.
>
> MAINTENANCE
>
> Restrictions on the maintenance of information systems used by Federal agencies, State and local governments, and other organizations include requirements that all information in these systems be accurate, complete, timely, and pertinent. Any individual has the right to inspect the information maintained in a system relating to him with the exception of medical records. He has the right to know the nature of the source and the recipients of that information. The individual also has the right to challenge any information on the basis of its accuracy, completeness, timeliness, pertinence, or necessity. Upon receipt of any challenge to its information by an individual, an organization must: First, investigate and record the current status of such information; second, purge any information that is found to be incomplete, not pertinent, not timely, not necessary to be maintained, or that can no longer be verified."

[21] §552a(c)(3)-(4),(d) §552a(e)(4)(I), §552a(f).
[22] §552a(e)(4)(g)-(h).
[23] §552a(g).

agency; to collect directly from the individual when they may result in adverse results to the individual; to inform that individual about the data collection and the effects of that collection; and to notify the public in the Federal register agency procedures about individual data collection notification and the sources of the records.[24]

The FBI sets forward no reason that it should be able to maintain records irrelevant or unnecessary to accomplish a purpose of the agency. Furthermore, the categories of sources of records at minimum are essential in order to keep the government accountable throughout their data collection and law enforcement activities. The exemptions as currently proposed are needlessly overbroad.

A purpose of the Privacy Act is to ensure that the information held about people is accurate, and that they know what information that is. For a database holding sensitive details of people's lives used for the purposes of investigation and law enforcement, upholding these tenets should be essential, the reason it was required by law. Any minor inaccuracy in data entered into the NCIC for any cause is spread across the country to various forms of law enforcement, and the effects of mistakes are exacerbated. Inaccurate NCIC records can impact the civil rights of an individual – and these exemptions which prevent individuals from being aware of and refuting inaccurate information exacerbate the risk of negative impacts. The NCIC has been known to have inaccurate and unreliable records[25], making it particularly unsuitable for vast exemptions from regulations designed to protect and optimize the accuracy and reliability of information held on people.

[24] §552(e)(1)-(3), (4)(g)-(i).
[25] EPIC Letter to OMB Director Joshua B. Bolten Re: NCIC Accuracy Concerns (February 20, 2004) https://www.epic.org/privacy/ncic/NCIC_letter.pdf.

Conclusion

The exemptions sought by the FBI of records in NCIC are contrary to the purpose of the Privacy Act. They will lead to increasing record inaccuracy and the misuse of personal information. They should be withdrawn.

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Jeramie D. Scott*
Jeramie D. Scott
EPIC Senior Counsel

/s/ *Ben Winters*
Ben Winters
EPIC Equal Justice Works Fellow