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

White House Office of Science and Technology Policy

RFI on Criminal Justice Statistics

88 Fed Reg. 10,150

March 30, 2023

The Electronic Privacy Information Center (EPIC) submits these comments in response to White House Office of Science and Technology Policy's (OSTP) February 16, 2023 Request for Information on Criminal Justice Statistics.[1] OSTP is preparing a report on "on the current data collection, use, and data transparency practices with respect to law enforcement activities."[2]

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to protect privacy, freedom of expression, and democratic values in the information age. Our mission is to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. EPIC has long called for bans on law enforcement use of facial recognition technology and for clear limitations, transparency, and accountability in jurisdictions that do not ban

[1] 88 Fed. Reg. 10,150, https://www.federalregister.gov/documents/2023/02/16/2023-03260/request-for-information-criminal-justice-statistics.
[2] *Id*.

its use.[3] EPIC regularly submits amicus briefs and engages with state and federal law enforcement agencies to better protect personal data and reduce the chances of law enforcement misuse of data.[4]

In these comments, EPIC has compiled a reading list of relevant work by EPIC and other organizations describing how law enforcement agencies regularly violate open records law, eschew transparency, and misuse data and statistics in ways that perpetuate harm.

EPIC urges OSTP to recognize that the widespread failure of law enforcement agencies to meaningfully comply with transparency and open records requirements is not due to lack of resources. Law enforcement agencies regularly decide not to prioritize spending on open records staff and actively fight disclosure and transparency. OSTP should not recommend federal funding for SLTT agencies to develop open records and transparency programs, but rather should push agencies to redirect more of their existing resources towards complying with transparency obligations.

EPIC also urges OSTP to consider how data collection and processing can be harmful, particularly to vulnerable individuals and marginalized communities. More data transfers between agencies are not necessarily safe or helpful. Where agencies do use personal data, privacy enhancing

[3] See, e.g., Ban Face Surveillance, EPIC Campaign, details available at https://epic.org/banfacesurveillance/; Testimony of EPIC, Massachusetts Joint Committee on the Judiciary (Oct. 22, 2019), https//epic.org/testimony/congress/EPIC-FacialRecognitionMoratorium-MA-Oct2019.pdf; EPIC, Civil Rights Concerns Regarding Law Enforcement Use of Face Recognition Technology, Coalition Letter (June 3, 2021), https://epic.org/privacy/facerecognition/Civil-Rights-Statement-of-Concerns-LE-Use-of-FRT-2021.pdf; EPIC, Letter to President Biden on Implementing a Facial Recognition Technology Moratorium, Coalition Letter (Feb. 16, 2021), https://epic.org/privacy/facerecognition/Coalition-Letter-Biden-FRT-Moratorium.pdf, Comments of EPIC to the Office of the Privacy Commissioner of Canada re: Privacy guidance on facial recognition for police agencies (Oct. 15, 2021), https://epic.org/documents/draft-guidance-to-canadian-police-agencies-on-facial-recognition/.

[4] *See e.g.*, Sharpe v. Winterville Police Department No. 21-1827 (2021), Brief of EPIC as Amicus Curie, https://epic.org/documents/sharpe-v-winterville-police-department/; Dana Khabbaz, DHS's Data Reservoir: ICE and CBP's Capture and Circulation of Location Information, EPIC (Aug. 2022), https://epic.org/documents/dhss-data-reservoir-ice-and-cbps-capture-and-circulation-of-location-information/; EPIC Comments to the NYPD on POST Act Disclosures (Feb. 25, 2021), https://epic.org/documents/nypd-post-act-disclosures/.

technologies including differential privacy should be employed to protect highly sensitive personal information from being exposed.

I. Law Enforcement Failures to Meaningfully Respond to Public Records Requests and Transparency Obligations:

1. Krista Johnson, *Louisville Metro Police Department illegally withholding, destroying records, group says*, Louisville Courier-J. (Oct. 6, 2022), https://www.courier-journal.com/story/news/local/2022/10/06/louisville-police-breaking-open-records-laws-490-project-lawsuit-says/69536201007/.

2. Rebecca Heilweil, *Why we don't know as much as we should about police surveillance technology*, Vox (Feb. 5, 2020), https://www.vox.com/recode/2020/2/5/21120404/police-departments-artificial-intelligence-public-records.

3. Eleni Manis & Albert Fox Cahn, *ABOVE THE LAW? NYPD Violations of the Public Oversight of Surveillance Technology (POST) Act*, S.T.O.P. (Oct. 7, 2021), https://www.stopspying.org/above-the-law.

4. EPIC Comments to the NYPD on POST Act Disclosures (Feb. 25, 2021), https://epic.org/documents/nypd-post-act-disclosures/.

5. Postal Service Fails to Conduct Privacy Impact Assessment for internet Covert Operations Program (iCOP)

    a. *EPIC v. USPS*, No. 21-2156 (DDC 2021), https://epic.org/documents/epic-v-u-s-postal-service/.

    b. USPS Office of Inspector General, Report Number 21-191-R22, *U.S. Postal Inspection Service's Online Analytical Support Activities* (Mar. 25, 2022), https://www.uspsoig.gov/sites/default/files/reports/2023-01/21-191-R22.pdf.

6. *Shining a Light on New Jersey's Secret State Intelligence System,* Rutgers Ctr. for Sec., Race, & Rights (Mar. 2023), https://csrr.rutgers.edu/wp-content/uploads/2023/03/intelligence-report.pdf.

II. Harmful Uses of Statistical Data for Policing

Statistical data has been used for over 30 years to justify targeted policing practices that harm marginalized communities without contributing to public safety. The history of data abuse is key context for any attempt to use data for purportedly good aims.

1. Andrew Guthrie Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (2017).

2. Peter Hanink, *Don't Trust the Police: Stop Question Frisk, CompSTAT, and the High Cost of Statistical Over-reliance in the NYPD*, ResearchGate (Aug. 2018), https://www.researchgate.net/publication/327189605_Don%27t_trust_the_police_Stop_question_frisk_COMPSTAT_and_the_high_cost_of_statistical_over-reliance_in_the_NYPD

    a. Reply All, *The Crime Machine (#127)* (Oct. 12, 2018), https://gimletmedia.com/shows/reply-all/o2hx34/.

3. Sara Brayne, *Predict and Surveil: Data, Discretion, and the Future of Policing* (2020)

III. Impact of Collecting and Disseminating Intrusive Data on Vulnerable Populations

Victims of crime shouldn't have to feel like they're being asked to decide whether to (1) give up their privacy or (2) receive services.

1. National Network to End Domestic Violence, *Why Privacy and Confidentiality Matters for Victims of Domestic & Sexual Violence*, https://www.techsafety.org/privacymatters (noting that survivors of domestic violence may opt for homelessness or going without an ID rather than risk having their info in a database where it may be discovered).

2. Prof. Khiara Bridges addressed a similar privacy-or-services dynamic for poor mothers in *The Poverty of Privacy Rights*, https://www.sup.org/books/title/?id=25115

3. EPIC Comments to the FCC on Location-Based Routing for 911 Calls (Feb. 16, 2023), https://epic.org/epic-urges-fcc-to-safeguard-precise-911-location-data-before-mandating-collection/ (misuse of emergency location data)

4. EPIC's Response to Reports of Crisis Text Line's Policies (Jan. 31, 2022), https://epic.org/epics-response-to-reports-of-crisis-text-line-data-policies/ (recipients of services may feel betrayed to learn their data was used for other purposes, having a chilling effect on use of services)

    1. @BrendanCarrFCC (Jan. 31, 2022, 9:21 PM), https://twitter.com/BrendanCarrFCC/status/1488336797449007111 ("The success of the Lifeline, and other mental health hotlines, is directly tied to the public's trust that conversations will remain confidential. In fact, one of the reasons people in crisis do not call the Lifeline or otherwise seek help is because they are worried that they might lose their anonymity.")

    2. Keris Myrick, Comments at FCC Forum on Geolocation for 988 at 3:19:24, https://youtu.be/HjHXXPGEuus?t=11964s ("[W]e [people with lived experience, suicide attempt survivors and their family members] also need to know who owns the data and how is it being shared?"); *id.* at 3:22:16, https://www.youtube.com/watch?v=HjHXXPGEuus&t=12136s (individuals from communities experiencing disproportionate institutionalization may be reluctant to trust that systems that use geolocation data will help them and not harm them)

5. Comments of EPIC et al to DHHS on HIV Prevention Medication Distribution Records (Feb. 22, 2023), https://epic.org/epic-coalition-urge-hhs-to-abandon-database-tracking-hiv-prep-users%ef%bf%bc/ (addressing privacy and safety risks created by database collecting information from vulnerable populations including LGBTQ individuals, Black and Brown individuals, undocumented immigrants, and low-income individuals)

IV. Privacy Enhancing Technologies as Minimum Safeguards

1. EPIC Comments to OSTP on Advancing Differential Privacy (Jul. 8, 2022), https://epic.org/documents/epic-comments-to-ostp-on-advancing-differential-privacy/

2. EPIC Comments to NIST on NIST De-Identifying Government Data Sets Paper (3rd Draft) (Jan. 13, 2023), https://epic.org/documents/epic-comments-on-nist-de-identifying-government-data-sets-paper-3rd-draft/.

V. Conclusion

EPIC urges OSTP to take a privacy-focused approach to criminal justice statistics and recognize that many uses of such statistics do more harm than good. We reiterate that the failures of law enforcement agencies to produce and publicize statistics do not reflect a pure lack of resources, but rather deliberate choices not to invest in transparency and public records infrastructure. Police departments should not be rewarded with more federal funds for systematic failures to comply with existing obligations. And all law enforcement agencies should be particularly careful with respect to the personal data of survivors of domestic violence and other vulnerable populations. At a minimum, departments should require differential privacy and other data protection techniques before publishing or making available datasets containing particularly sensitive information. For further questions or input, please reach out to EPIC Counsel Jake Wiener at wiener@epic.org.

Respectfully Submitted,

Jake Wiener
Jake Wiener
EPIC Counsel

Chris Frascella
Chris Frascella
EPIC Law Fellow