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

joined by the

Center for Digital Democracy and Consumer Federation of America

to the

Office of Science and Technology Policy

Regarding the

Public and Private Sector Uses of Biometric Technologies

January 15, 2022

The Electronic Privacy Information Center ("EPIC") submits the following feedback to the request for information by the Office of Science and Technology Policy ("OSTP") on the public and private sector uses of biometric technologies.[1] We submit these comments to 1) stress the importance of robust, timely, and transparent impact assessments to mitigate the privacy and human rights risks of biometric technologies; 2) highlight the need for rigorous impact assessments that broadly consider the potential impact and apply to all biometric technologies; and 3) articulate key factors impact assessments should consider.

EPIC is a public interest research center in Washington, D.C. 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.[2] EPIC has a long history of promoting transparency and accountability of the technologies used in the private and public sectors.[3]

EPIC has a particular interest in promoting transparency and accountability regarding the use of biometric technologies and has consistently advocated for the need for safeguards related to the use

[1] Notice of Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies, 86 Fed. Reg. 56,300 (Oct. 8, 2021), https://www.govinfo.gov/content/pkg/FR-2021-10-08/pdf/2021-21975.pdf.
[2] EPIC, *About EPIC* (2022), https://epic.org/about/.
[3] EPIC, *Algorithmic Transparency* (2018), https://www.epic.org/algorithmic-transparency/; EPIC, *Algorithms in the Criminal Justice System* (2018), https://www.epic.org/algorithmic-transparency/crim-justice/; Comments of EPIC, *Consumer Welfare Implications Associated with the Use of Algorithmic Decision Tools, Artificial Intelligence, and Predictive Analytics*, Federal Trade Commission (Aug. 20, 2018), https://epic.org/apa/comments/EPIC-FTC-Algorithmic-Transparency-Aug-20-2018.pdf; Comments of EPIC, *Developing UNESCO's Internet Universality Indicators: Help UNESCO Assess and Improve the Internet*, United Nations Educational, Scientific and Cultural Organization ("UNESCO") (Mar. 15, 2018), 5-6, https://epic.org/internetuniversality/EPIC_UNESCO_Internet_Universality_Comment%20(3).pdf.

of biometric technologies as well as the need to ban certain technologies or specific uses of those technologies. EPIC, through the Public Voice coalition, gathered support from over 100 organizations for a declaration calling for a moratorium on the further deployment of facial recognition for mass surveillance.[4] More recently, EPIC joined an open letter calling for a global ban on biometric recognition tools used for mass and discriminatory surveillance.[5]

I. Robust, timely, and transparent impact assessments are necessary to mitigate the privacy and human rights risks of biometric technologies.

Like all systems that collect and process personal data, it is imperative that biometric technologies only be introduced—if at all—after a robust and transparent review of the resulting risks to privacy and human rights. The process of evaluating technologies before their potential use is known as an impact assessment (or risk assessment).[6] An impact assessment is an analysis of how personally identifiable information will be collected, processed, stored, and transferred.[7] Properly executed, an impact assessment forces an entity to identify privacy and human rights risks of a proposed technology or application of a technology; to determine how and if those risks should be mitigated; and to make an informed decision whether the technology or application can be justified in light of its impact.[8] Impact assessments are mandated by numerous legal frameworks, including the E-Government Act of 2002,[9] the European Union's General Data Protection Regulation,[10] and the California Privacy Rights Act of 2020.[11]

It is essential that impact assessments for biometric technologies operate as true decision points and not as box-checking exercises used to legitimize foregone conclusions. As Professor Gary T. Marx writes, the object of a privacy risk assessment is to "anticipate[] problems, seeking to prevent, rather than to put out fires."[12] Accordingly, an impact assessment "is a process which should begin at the earliest possible stages, when there are still opportunities to influence the outcome of a project."[13] Moreover, an impact assessment "is not a time-restricted activity that is limited to a particular milestone or stage of the information system," but rather "shall continue throughout the information system and PII life cycles" and must be updated whenever circumstances "alter the privacy risks

[4] https://thepublicvoice.org/ban-facial-recognition/.

[5] Access Now et al., *Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance* (2021), https://www.accessnow.org/cms/assets/uploads/2021/06/BanBS-Statement-English.pdf.

[6] EPIC, *Privacy Impact Assessments* (2021), https://epic.org/issues/open-government/privacy-impact-assessments/.

[7] *Id.*

[8] *Id.*

[9] E-Government Act, Pub. L. No. 107-347, § 208, 116 Stat. 2899, 2921–23 (Dec. 17, 2002) (codified at 44 U.S.C. § 3501 note).

[10] Commission Regulation (EU) 2016/679, art. 35, 2016 O.J. (L 119).

[11] Cal. Civ. Code § 1798.185(a)(15).

[12] *Privacy Impact Assessment* at v (David Wright & Paul de Hert, eds., 2012).

[13] *Id.* at 5–6; *see also* Office of Mgmt. & Budget, *OMB Circular A-130: Managing Information as a Strategic Resource* (2016), app. II at 10, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf ("Agencies shall conduct and draft a PIA with sufficient clarity and specificity to demonstrate that the agency fully considered privacy and incorporated appropriate privacy protections from the earliest stages of the agency activity and throughout the information life cycle.").

associated with the use of such information technology."[14] At all stages of this process, one realistic outcome of an assessment must be an institutional decision to substantially modify or abandon a proposed use of biometric technology based on the privacy and human risks it would pose.

Indeed, some forms of biometric technology—those who core functionality rests on invasive, nonconsensual, and unaccountable processing of biometric data—could not survive a robust impact assessment at all. For example, the privacy and human rights risks of emotion recognition systems cannot be justified or mitigated in view of the accuracy, bias, and privacy risks they carry.[15] So too with mass biometric surveillance tools,[16] including face surveillance.[17] It is essential that impact assessments be conducted early and with sufficient bite to prevent such biometric technologies from being deployed in the first place.

In many cases, an impact assessment also serves to inform the public of a data collection or system that poses a threat to privacy and human rights.[18] Requiring the prompt disclosure of impact assessments for biometric technologies will help ensure that each institution conducts a sufficiently rigorous evaluation of privacy and human rights risks; force the institution to justify the decision to introduce a given biometric technology; place the public on notice of the technology and how it will be used; and enable individuals and policymakers to respond to the technology before it deployed.

II. Impact assessments should apply to all biometric technologies and broadly consider the impact of the technology with thorough and detailed analysis.

Impact assessments should be triggered in all instances where biometric technologies are or will be used. Current implementations of biometric technologies should not be grandfathered in and thus allowed to avoid the requirement for an impact assessment. Similarly, seemingly non-controversial implementations of biometric technologies should not be exempt from an impact assessment requirement. A requirement for an impact assessment should avoid loopholes and exemptions that allow certain biometric technologies to avoid an assessment. A broad requirement that applies to all biometric technologies, including current as well as seemingly non-controversial biometric technologies, is more likely to identify potential issues.

The impact assessment requirement should extend to both the public and private sectors. Both government entities and private companies use biometric technologies and will no doubt look to expand their use of these technologies. Both sectors use biometric technologies in ways that create privacy, civil liberties, and human rights risks; disproportionately impact marginalized communities;

[14] Office of Mgmt. & Budget, *supra* note 13, at 10.
[15] *See* EPIC, *Feedback from: The Electronic Privacy Information Center (EPIC)*, European Commission ¶ 3 (Aug. 6, 2021).
[16] *See, e.g.*, Access Now, EPIC, et al., *Open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance* (2021), https://www.accessnow.org/cms/assets/uploads/2021/06/BanBS-Statement-English.pdf.
[17] *See* EPIC, *Ban Face Surveillance* (2022), https://epic.org/campaigns/ban-face-surveillance/.
[18] *See, e.g.*, E-Government Act § 208(b)(1)(B)(iii) (requiring the publication of impact assessments by federal agencies).

and create opportunities for abuse.[19] The obligation to conduct an impact assessment should fall on all entities that use biometric technologies, including those entities that merely use a service that involves a biometric technology provided by a third party. For example, each law enforcement agency that uses the controversial facial recognition service provided by Clearview AI should be required to conduct an impact assessment in addition to Clearview AI itself.[20] Similarly, each airline and airport that uses the Traveler Verification Service that identifies travelers through facial recognition system managed by Customs and Border Protection should be required to conduct their own impact assessment before using the service.[21]

An impact assessment should be a thorough examination of the biometric technology at issue and include a serious analysis of the potential impact of the technology prior to its potential implementation. Too often an assessment requirement lacks teeth and becomes merely a lower priority box to check—one that is frequently checked after the fact instead of prior to the implementation of the biometric technology. This has often been the case with the privacy impact assessment requirement of the E-Government Act of 2002, particularly as it applies to the use of facial recognition technology.

The E-Government Act of 2002 requires government agencies to conduct a privacy impact assessment ("PIA") prior to "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form."[22] Despite this requirement, PIAs are often conducted after the fact if at all. Additionally, PIAs tend to narrowly construe the potential issues the technology raises and focus on justifying the technology instead of an honest analysis of its impact and whether the technology should be implemented.

For example, Immigration and Customs Enforcement ("ICE") began using the facial recognition services of Clearview AI almost a year prior to the completion of a relevant PIA in May 2020.[23] It's clear from the documents obtained by EPIC through the Freedom of Information Act that the DHS Privacy Office, which is generally responsible for making sure PIAs are conducted, was not initially aware that ICE was using Clearview, only asking to be briefed on its use in December 2019.[24]

[19] *See* Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. Times (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html; *see also*, Kashmir Hill, *Before Clearview Became a Police Tool, It Was a Secret Plaything of the Rich*, N.Y. Times (Mar. 5, 2020), https://www.nytimes.com/2020/03/05/technology/clearview-investors.html;

[20] Clearview AI is a controversial facial recognition service that scrapes billions of photos from websites to create a massive biometric database used by hundreds law enforcement agencies. *See* Ryan Mac, Caroline Haskins, *et al.*, *How A Facial Recognition Tool Found Its Way Into Hundreds Of US Police Departments, Schools, And Taxpayer-Funded Organizations*, Buzzfeed News (), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition.

[21] As part of the Biometric Entry-Exit program that uses facial recognition to verify the identity of travelers entering and leaving the country, Customs and Border Protection created the Traveler Verification Service, which can also be used by airlines to verify a traveler's identity during, for example, baggage check.

[22] E-Government Act § 208(b)(1)(A)(i).

[23] Ryan Mac, Caroline Haskins, and Logan McDonald, *Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's Walmart, and the NBA* (Feb. 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

[24] Email re: Clearview PTA (December 3, 2019) (obtained through the Freedom of Information Act), https://epic.org/wp-content/uploads/2022/01/EPIC-20-03-06-ICE-FOIA-Email-Clearview-PTA.pdf.

The PIA conducted by DHS regarding ICE's use of facial recognition services, specifically Clearview AI, lacks a meaningful assessment of the risks of a facial recognition database of billions of images indiscriminately scraped from the internet. The focus of the facial recognition services PIA is on ICE's handling of the photos the agency submits to Clearview AI or other providers of facial recognition services for searches and the results the agency gets back. The few impacts that the facial recognition services PIA does mention that are specifically created by Clearview AI's facial recognition database are chalked up as a "risk [that] is not mitigated" and more or less left at that. These unmitigated risks appear to serve no role in determining whether ICE should use such a service. Indeed, the facial recognition services PIA is not focused on whether Clearview should be used only on what the agency is doing to mitigate the narrow set of risks ICE is willing to address.

Another issue federal government PIAs tend to ignore, particularly with the use of facial recognition, is the disproportionate impact and racial bias inherent in these systems. For example, the Federal Bureau of Investigation conducted a PIA for its Next Generation Identification ("NGI") database that contains various biometric modalities, including images for facial recognition.[25] The images in the database that are used in facial recognition searches come from mugshots. It is well known that the criminal justice system disproportionately arrests and incarcerates Black people. Consequently, Black people are over-represented in NGI database of facial recognition photos. Additionally, facial recognition systems tend to be the least accurate on Black people. The PIA does nothing to address the issues created by using a system that has historic racial bias built into it. It is imperative that an impact assessment requirement necessitate the broad consideration of the impact of the biometric technology and thorough evaluation of the issues the technology raises.

III. Impact assessments should, at a minimum, consider several key factors related to the collection, use, dissemination, and retention of biometric data.

Although impact assessments should not be one-size-fits-all box-checking exercises, there are certain essential factors and categories an impact assessment must address. When assessing the impacts of biometric systems, the data at issue will always be sensitive.

Impact assessments must be sufficiently detailed and should consider several factors related to the collection, use, dissemination, and retention of biometric data.[26] The assessments should be able to generally indicate what type of regulatory intervention is appropriate for a given system.

Both the content and process of the impact assessment tool are hugely impactful. The assessments must be published, performed by someone with the requisite access and understanding of a given tool, and be legitimized through threats of fine or disgorgement if the assessment registers sufficient risk or is done inadequately.[27]

[25] FBI, *Privacy Impact Assessment for the [Next Generation Identification-Interstate Photo System*, (Oct. 29, 2019), https://www.fbi.gov/file-repository/pia-ngi-interstate-photo-system.pdf/view.

[26] *See* Dillon Reisman, Jason Schultz, Kate Crawford, Meredith Whitaker, *Algorithmic Impact Assessments: A practical framework for public agency accountability,* AI Now Institute (April 2018), https://ainowinstitute.org/aiareport2018.pdf.

[27] *Commission Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM(2021) 206 final (Apr. 21, 2021).

EPIC urges that impact assessments address the following minimum factors to prevent mission and function creep, needless over-collection of biometric data, and non-consensual processing of data:[28]

- Mission and function creep:[29] The stated purpose of the system, the allowable uses of the system, and the justification for adopting the system.
- Needless over-collection of data:[30] Information about the data collected for or by a system, including but not limited to the purpose for collection and the source(s) of the data.
- Lack of consent:[31] Information about data collection methods, including the scope of consent obtained (if any) and limitations on scraping.
- Failure to minimize:[32] Information about the management, retention, deletion, and transfer of data.
- Lack of transparency:[33] Information about the logic and development of a system.
- Lack of due diligence:[34] Initial tests regarding the accuracy and propriety of a system and information about ongoing tailored testing of a system. In addition to accuracy and propriety, audits and impact assessments must center civil rights, specifically testing for disproportionate impact based on race or other protected classes.
- Lack of accountability:[35] Any appeal procedures or harm mitigation strategies employed and information about key players, including the developer of a system, the user of a system, and the evaluators of the system.

In a growing number of countries, automated decisionmaking systems—including those that process biometric data—are required to undergo impact assessments. In Canada, for example, businesses input information about automated decisionmaking systems into a standardized survey, which allows for the evaluation of system based on design attributes, the sensitivity of data processed, and the system's connection to areas requiring additional considerations and protections.[36] This type of form could be used to collect and ensure uniform reporting of key information about biometric technologies and systems. The Canadian assessment asks each business to evaluate the stakes of the decisions that a system makes, the vulnerability of subjects, and whether the system is a predictive tool.[37] The tool also allows for multiple answer options and detailed explanations of responses. In

[28] *See* EPIC's comments on the California Privacy Rights Act (particularly the "scope of risk assessments" section, https://epic.org/documents/comments-of-epic-and-three-organizations-on-regulations-under-the-california-privacy-rights-act-of-2020/.

[29] *See, e.g.*, Arif Kornweitz, *A New AI Lexicon: Function Creep*, AI Now Institute (Aug. 4, 2021), https://medium.com/a-new-ai-lexicon/a-new-ai-lexicon-function-creep-1c20834fab4a.

[30] *See, e.g.*, Olivia Solon, *Facial Recognition's dirty little secret: millions of online photos scraped without consen*t, NBC News (Mar. 12, 2019), https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921.

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] Necessary in large part because of demonstrated lack of accuracy and bias. *See, e.g.* Joy Buolamwini, Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,* Fairness Accountability and Transparency Conference (Feb. 2018), https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[35] *Id*.

[36] Canada Digit. Servs., *Algorithmic Impact Assessment* (2021), https://open.canada.ca/aia-eia-js/?lang=en.

[37] *Id*.

some cases, the Canadian tool requires a business to identify the downstream processes of a system. This includes asking (1) whether the system will only be used to assist a decision-maker; (2) whether the system will be making a decision that would otherwise be made by a human; (3) whether the system will be replacing human judgment; (4) whether the system will be used by the same entity that developed it; and (5) for details about the system's economic and environmental impacts.[38]

Although impact assessments can't be the sole regulatory mechanism governing biometric systems, robust impact assessments *combined* with a system of governance that incorporates oversight and protects privacy and human rights can help regulators manage the risks that biometric technologies pose.

IV. Conclusion

We thank OSTP for the opportunity to comment on the use of biometric technologies and urge the agency to push for a meaningful impact assessment requirement as described in this comment. We look forward to working with OSTP in the future on these issues.

Respectfully Submitted,

/s/ Jeramie Scott
Jeramie Scott
EPIC Senior Counsel

/s/John Davisson
John Davisson
EPIC Senior Counsel

/s/Ben Winters
Ben Winters
EPIC Counsel

[38] *Id*.