
*Comments of the World Privacy Forum to U.S. Citizenship and Immigration Services, Department of Homeland security*
*regarding*
*Collection and Use of Biometrics by U.S. Citizenship and Immigration Services, NPRM, U.S. Citizenship and Immigration Services, Department of Homeland Security, USCIS Docket No. USCIS-2019-0007*

*Sent via regulations.gov and copied via email to DHSDeskOfficer@omb.eop.gov*

Michael J. McDermott,
Security and Public Safety Division,
Office of Policy and Strategy,
U.S. Citizenship and Immigration Services,
Department of Homeland Security,
20 Massachusetts Ave. NW,
Washington, DC 20529-2240

**October 13, 2020**

**RE: World Privacy Forum comments regarding Collection and Use of Biometrics by U.S. Citizenship and Immigration Services NPRM, U.S. Citizenship and Immigration Services, Department of Homeland Security, USCIS Docket No. USCIS-2019-0007**

Dear Mr. McDermott,

The World Privacy Forum is pleased to provide comments regarding the Notice of Proposed Rulemaking 85 FR 56338, available at: https://www.govinfo.gov/content/pkg/FR-2020-09-11/pdf/2020-19145.pdf.

The World Privacy Forum (WPF) has standing and expertise to respond to this NPRM. WPF has conducted meaningful work in the area of biometrics, including now more than

10 years of research which includes substantive field research with national-level biometrics systems. We have published peer-reviewed research regarding biometrics, including original research in Nature-Springer and Harvard-based Journal of Technology Science [See: ***A Failure to Do No Harm: India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.*** , Pam Dixon, Springer Nature, Health Technology. DOI 10.1007/s12553–017-0202-6. http://rdcu.be/tsWv. Open Access, via Harvard-Based *Journal of Technology Science*: https://techscience.org/a/2017082901/. ] Additionally, we have published and presented extensive work on biometric policy, including presentations at the Harvard Kennedy School [See: ***Digital Identity Ecosystems***, 4 February 2019, https://www.worldprivacyforum.org/2019/02/digital-identity-ecosystems/, , and policy research such as ***Expanding Solutions to Address the Risks of Face Recognition Systems,*** 3 September 2020: https://www.worldprivacyforum.org/2020/09/expanding-solutions-to-solve-risks-of-face-recognition-systems/.] WPF is a member in good standing of the advisory board of the Biometrics Institute and a member of the Biometric Institute Privacy Experts Group.

## I. Overview of Problems in the DHS NPRM

In overview, WPF finds the DHS proposal to lack scientific basis, particularly in its omission of known facts and policies that, if included, would contravene the proposal. WPF finds that the DHS NPRM has avoided discussion of the new barriers it creates for vulnerable populations, including victims of crimes such as human trafficking, among others. Further, the DHS proposal outlines a significant expansion of the utilization of biometrics[1] for individuals of all ages, including children and infants, a collection which is scientifically questionable and fraught with ethical questions and problems.

The NPRM lacks substantiation for its proposed rulemaking. It states: "The proposed rule would provide benefits that are not possible to quantify." The U.S. government should not, and must not, be in the business of promulgating rules that cannot be quantified, and that do not provide quantifiable, measurable benefit to the people the rule(s) impact. To have a legitimate rule, DHS must put forward a proposal with full substantiation of its necessity, impact, and risks.

DHS's asserts one of the benefits of its NPRM is that its proposal for a significantly expanded collection of biometrics is necessary to thwart identity theft and fraud, when it is well-documented that biometrics are themselves subject to various forms of fraud and

---

[1] In this comment, *biometric* refers to automated recognition of individuals based on their biological and/or behavioral characteristics. There are many types of biometrics. For example facial recognition systems are a type of biometric, as are systems that include fingerprint analysis, iris recognition, and gait analysis. See: International Organization for Standardization: Information technology, Vocabulary, Part 37: Biometrics. ISO/IEC 2382-37:2017, JTC 1/SC 37, Geneva, Switzerland, 2017. Available at: https://www.iso.org/standard/66693.html.

new forms of biometric identity theft,[2] an issue DHS has chosen to neglect in this NPRM. Both a discussion and documentation of the risk of biometric morphing, spoofing, identity theft and the risk of biometric data breach[3] resulting from the expanded biometric collection that would result if the NPRM goes into effect has been entirely omitted from the NPRM. There are many additional substantive problems in the NPRM.

Problems in this NPRM include:

- This NPRM contains abrogations of the *United Nations Convention Against Transnational Organized Crime and the Protocols Thereto* (The Palermo Convention), including Article 24, Protection of Witnesses, as well as Annex II.[4]
- This NPRM contains abrogations of the Council of Europe's *Convention on Action against Trafficking in Human Beings,* specifically, Article 11 regarding the protection of private life. The Council of Europe, Warsaw, 16.V.2005.[5]
- The NPRM definition of "biometric" does not conform to the internationally accepted definition from the International Organization for Standardization: Information technology, Vocabulary, Part 37: Biometrics. ISO/IEC 2382-37:2017, JTC 1/SC 37, Geneva, Switzerland, 2017.

---

[2] Pam Dixon, *A Failure to Do No Harm: India's Aadhaar biometric ID program and its inability to protect privacy in relation to measures in Europe and the U.S.* (Pam Dixon, Springer Nature, Health Technology. DOI 10.1007/s12553–017-0202-6. http://rdcu.be/tsWv. Open Access, via Harvard-Based Technology Science: https://techscience.org/a/2017082901/. See discussion of biometric identity theft (via biometric template takeover and spoofing) under "consent and biometrics."

3 Biometric data breach is when biometric templates or other biometric data have been acquired through unauthorized access. See, for example, two articles about the Suprema BioStar 2 data breach: Report: Data breach in Biometric Security Platform Affecting Millions of Users, vpnMentor, August 2019, https://www.vpnmentor.com/blog/report-biostar2-leak/. See also: Biometric Data Breach: database exposes fingerprints, face recognition data of 1 million people, Norton Security Center, Emerging Threats, August 2019. https://us.norton.com/internetsecurity-emerging-threats-biometric-data-breach-database-exposes-fingerprints-and-facial-recognition-data.html.

[4] *United Nations, Palermo Convention*, 2004. https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf

[5] *Convention on Action against Trafficking in Human Beings*, The Council of Europe, Warsaw, 16.V.2005. Available at: http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/090000168008371d See: "Article 11 – Protection of private life 1.) Each Party shall protect the private life and identity of victims. Personal data regarding them shall be stored and used in conformity with the conditions provided for by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). 2.) Each Party shall adopt measures to ensure, in particular, that the identity, or details allowing the identification, of a child victim of trafficking are not made publicly known, through the media or by any other means, except, in exceptional circumstances, in order to facilitate the tracing of family members or otherwise secure the well-being and protection of the child."

- The programs described in this NPRM do not conform to Fair Information Practices, which they must do to be in compliance with Executive Order 13,768.[6]
- This NPRM proposes the collection of biometrics for all ages, even infants. Yet it neglects to discuss the well-documented inaccuracies of biometrics for people at the younger and the older ranges of the age spectrum. In the landmark NIST study by Patrick Grother, Mei Ngan, and Kayee Hanaoka, (Face Recognition Vendor Test [FRVT] Part 3: *Demographic Effects in Facial Systems*, NIST, December 2019) NIST wrote: "We found elevated false positives in the elderly and in children; the effects were larger in the oldest adults and youngest children, and smallest in middle aged adults. The effects are consistent across country-of-birth, datasets and algorithms but vary in magnitude." See pages 8, 17 and associated technical material.[7] These facts were not reckoned with in the NPRM.
- There is no discussion in the NPRM of the security risks of biometrics, which are myriad and vary depending on the biometric in discussion. For example, there is no discussion of biometric forms of identity theft, nor biometric template security, which is vulnerable to specific types of attacks.[8] Further, the NPRM contains no recognition of biometric spoofing,[9] a well-understood and significant security problem in biometrics. The NPRM also contains no

---

[6] An important history of the development of Fair Information Principles is Robert Gellman, A Basic History of Fair Information Practices. Available at: http://bobgellman.com/rg-docs/rg-FIPShistory.pdf and http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020

[7] Patrick Grother, Mei Ngan, Kayee Hanaoka. Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects in Facial Systems, NIST, December 2019. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf. See pages 8, 17 and associated technical material.

[8] Anil K. Jain, Karthik Nanakumar, and Abhishek Nagar. *Biometric Template Security*, EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics, January 2008. Available at: http://www.cse.msu.edu/~rossarun/BiometricsTextBook/Papers/Security/JainNandakumarNagar_TemplateSecuritySurvey_EURASIP08.pdf . *See also*:
Anil K. Jain, Arun A. Ross, and Karthik Nandakumar. Introduction to Biometrics. Springer: New York, London. Chapter 7, Security of Biometric Systems.

[9] Anil K. Jain, Arun A. Ross, and Karthik Nandakumar. Introduction to Biometrics. Springer: New York, London. Chapter 7, Security of Biometric Systems. See pp. 269-278.

recognition of, nor mitigations for, biometric morphing,[10] a serious security problem associated with certain types of biometrics.[11] The U.S. government has recognized these problems and has published scientific studies regarding these issues.[12]

- The NPRM contains no recognition of problems associated with the entire ecosystem of biometrics, for example, the hardware components of certain types of biometrics such as cameras in face recognition ecosystems, to name just one example.[13]
- The NPRM excludes discussion of the problems of demographic bias in certain types of biometric algorithms and ecosystems, which is now well-documented by NIST and others.[14]
- There is no discussion or substantiation of why expansion of biometric collections are the *only* answer to the problems DHS has presented. Alternative

---

[10] *Morphing* is a type of biometric presentation attack where biometric samples (such as photographs) of multiple individuals are merged, typically using photographic editing software. The final merged image can be comprised of 2 or more photos. The goal of a morphing attack is to allow a successful biometric verification of all contributing subjects against the final "morphed" identity. A high quality morphed image can be very difficult to detect. Morphing can occur in facial recognition or other biometrics systems. In this letter, we refer to morphing attacks on facial recognition systems. *See also:* International Organization for Standardization: Information Technology, Biometric presentation attack detection, Part 3: Testing and reporting. ISO/IEC FDIS 30107-3:2017, JTC 1/SC 37, Geneva, Switzerland, 2017.

[11] U. Scherhag et al. A. Bromme, C. Busch, A. Dantcheva, C. Rathgeb and A. Uhl, Eds. Biometric Systems under Morphing Attacks: Assessment of Morphing Techniques and Vulnerability Reporting. BIOSIG 2017, Lecture Notes in Informatics (LNI), Gesellschaft fur Informatik, Bonn 2017. Available at: https://christoph- busch.de/files/Scherhag-Methodology-BIOSIG-2017.pdf.

[12] Mei Ngan, Patrick Grother, and Kayee Hanaoka. Face Recognition Vendor Test MORPH Performance of Automated Facial Morph Detection and Morph Resistant Face Recognition Algorithms, Concept, Evaluation Plan and API, VERSION 1.1. NIST. Sept. 6, 2018. Available at: https://www.nist.gov/sites/default/files/documents/2018/09/07/frvt_morph_api_v1.1.pdf.

[13] The ecosystem of biometrics is well-studied. See, for example, Mumtazah et al, *Technical Issues and Challenges of Biometric Applications as Access Control Tools of Information Security*, International Journal of Innovative Computing, Information and Control ICIC International, Volume 8, Number 11, November 2012 pp. 7983–7999 http://www.ijicic.org/ijicic-ksi-13.pdf. See in particular sections on biometric system components and measurements.

[14] NIST describes and quantifies demographic differentials for contemporary face recognition algorithms in its landmark report, NISTIR 8280. In this report, NIST quantified demographic differences for nearly 200 face recognition algorithms from nearly 100 developers, using four collections of photographs with more than 18 million images of more than 8 million people. See: Patrick Grother, Mei Ngan, Kayee Hanaoka. *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, NIST, December 2019. https://doi.org/10.6028/NIST.IR.8280 or https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf. See also: Dr. John W. M. Campbell. ISO Technical Report, (ISO/IEC JTC-1 SC 37). Demographic Bias in Biometric Systems: Current Research and Applicable Standards, January 2017. Available at: http://cradpdf.drdc-rddc.gc.ca/PDFS/unc265/p805126_A1b.pdf.

procedures for accomplishing tasks in a better, safer, and more effective way were neither discussed nor substantiated in this NPRM.

- The NPRM does not provide factual support for assertions in the document regarding the incidence of identity theft and fraud, which comprise some of the key rationales for its biometric collection for all ages, including children and even infants. Why does the NPRM avoid discussion of how many people are victims of ID theft? What years did this happen? What regions were they coming from?
- The NPRM does not discuss biometric accuracy variability (false positive, false negative). This is a well-studied area of inquiry. Research documents that when inaccuracies in biometric systems occur at scale, scale effects occur and create non-trivial challenges.[15]
- The NPRM proposes an $85 fee for biometric services fee, to be incorporated into an underlying fee. This additional fee poses a meaningful barrier to individuals from lower income countries, some of which have a per capita GNI of $870 (Democratic Republic of the Congo). Niger, Malawi, among others have a GNI ranging from $990 to $1,500. In Albania, the average monthly wage is $379. (OECD.StatExtracts, UNECE.) It is unconscionable to require vulnerable individuals to pay an $85 biometric processing fee when this comprises a significant portion of an annual or monthly salary.
- And finally, the NPRM does not address concerns about how, if it implements this expansion of its biometric program, it will assist people who are victims of crimes and human trafficking to come forward. Victims of human trafficking are subject to profound shame, and identification through biometrics poses yet another — and potentially insurmountable - obstacle, particularly when biometrics will be applied to children of all ages.[16]

The DHS NPRM is unprecedented in its broad requests for change, based on no substantiation. Because DHS has produced an NPRM that does not contain a balanced, transparent, fact-based discussion of relevant substantive issues, and because it has not supported its requests with substantiation that is factual, accurate, transparent, and fair, and because this NPRM has not considered the harm it may inflict on vulnerable people nor how this would be mitigated within its expanded biometrics collection, and because

---

[15] Brian DeCann and Arun Ross, De-Duplication Errors in a Biometric System: An Investigative Study. Proc. of IEEE International Workshop on Information Forensics and Security (WIFS), (Guangzhou, China), November 2013. Available at: https://www.cse.msu.edu/~rossarun/pubs/DeCannRossDeDuplicationError_WIFS2013.pdf .

[16] On the matter of victims being hesitant to come forward, shame and privacy are interlinked. Austin argues that shame is a marker for that which should be kept private: "Although what is private is often difficult to define, easy cases include information associated with intimacy and secrecy that lead to stigmatization and shaming if exposed." Austin, Lisa M., Privacy, Shame and the Anxieties of Identity (January 1, 2012). Available at SSRN: https://ssrn.com/abstract=2061748 or http://dx.doi.org/10.2139/ssrn.2061748

this NPRM did not employ a clear ethical framework to guide its decision making, this NPRM does not meet the rigor necessary for it to move forward.

WPF urges DHS to rescind this NPRM in its entirety for the reasons stated above, and as discussed in these comments.

**II. The DHS NPRM, if put into effect, would violate sections of the UN *Palermo Convention.* Further, the NPRM does not follow the recommendations of the 2016 DHS OIG report regarding ICE and USCIS and human trafficking cases. The DHS NPRM would also violate sections of the Council of Europe's *Convention on Action against Trafficking in Human Beings***

The NPRM creates fresh barriers to victims of human trafficking, in contravention of the UN Palermo Convention and the 1016 DHS OIG report, *ICE and USCIS Could Improve Data Quality and Exchange to Help Identify Potential Human Trafficking Cases* and the Council of Europe's *Convention on Action against Trafficking in Human Beings.*

DHS' approach to victims of crime, by creating expanded mandatory biometric collections, including of children under 14, would violate Article 24 of the UN Palermo Convention by creating an environment of intimidation. We note that biometrics collection, depending on the biometric, can be an invasive and uncomfortable process. Even if the collection itself is not invasive, the idea of being biometrically identified and tracked is challenging for individuals who are already afraid. Notably, Article 24, *Protection of witnesses*, of the ***UN Convention Against Transnational Organized Crime and the Protocols Thereto*** (The Palermo Convention) states:

> 1. Each State Party shall take **appropriate measures within its means to provide effective protection from potential retaliation or intimidation for witnesses in criminal proceedings** who give testimony concerning offences covered by this Convention and, as appropriate, for their relatives and other persons close to them.
> 2. The measures envisaged in paragraph 1 of this article may include, inter alia, without prejudice to the rights of the defendant, including the right to due process:
>
> > (a) **Establishing procedures for the physical protection of such persons, such as, to the extent necessary and feasible, relocating them and permitting, where appropriate, non-disclosure or limitations on the disclosure of information concerning the identity and whereabouts of such persons;**
> > **(b) Providing evidentiary rules to permit witness testimony to be given in a manner that ensures the safety of the witness, such as permitting testimony to be given through the use of communications technology such as video links or other adequate means.**

> 3. States Parties shall consider entering into agreements or arrangements with other States for the relocation of persons referred to in paragraph 1 of this article.
> 4. The provisions of this article shall also apply to victims insofar as they are witnesses. [*emphasis added*]

The United States has ratified the Palermo Convention.[17]

As discussed, DHS' approach to victims of crime, by creating mandatory biometric collection, including of children and even infants, would violate Article 24 by creating an environment of intimidation. Few if any victims of crime and human trafficking are comfortable with mandatory biometric identification. The HHS fact sheet on *Identifying Victims of Human Trafficking* [18] notes that victims of human trafficking already suffer from significant distrust of authorities:

> A human trafficking victim may develop a mindset of fear, distrust, denial, and conflicting loyalties. Foreign victims of trafficking are often fearful of being deported or jailed and, therefore, they may distrust authority figures, particularly law enforcement and government officials. Similarly, traffickers may convince sex trafficking victims who are U.S. citizens or LPRs that, if they report their traffickers to the police, the police will jail the victim for prostitution while the traffickers, pimps, or johns will go free. Many victims of both sex and labor trafficking fear that if they escape their servitude and initiate investigations against their trafficker, the trafficker and his/her associates will harm the victims, the victims' family members, or others.

The NPRM's approach would exacerbate the problems HHS identified. In 2016, the DHS Office of the Inspector General (OIG) urged DHS to improve data quality and exchange to improve the plight of victims of trafficking. The OIG did not recommend mandatory, extensive collection of biometrics to do so.[19] In its report, however the OIG brought forward numerous problems unrelated to identification of individuals.

Of great concern in the OIG report is that according to USCIS data, fewer than 1,000 foreign national victims applied for "T visas" each year from 2005 to 2014. This is an extremely low number when compared with what OIG noted is the estimated "hundreds

---

[17] UN, Palermo Convention, Ratification Page: https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XVIII-12&chapter=18&clang=_en. Accessed 13 October, 2020.

[18] *Fact Sheet: Identifying Victims of Human Trafficking,* Administration for Children and Families, US Department of Health and Human Services, August 8 2012. https://www.acf.hhs.gov/archive/otip/resource/fact-sheet-identifying-victims-of-human-trafficking.

[19] DHS Office of the Inspector General, *ICE and USCIS Could Improve Data Quality and Exchange to Help Identify Potential Human Trafficking Cases,* Jan. 4, 2016. https://www.oig.dhs.gov/assets/Mgmt/2016/OIG-16-17-Jan16.pdf

of thousands of human trafficking victims in the United States," and the OIG further noted that this number is "..far below the 5,000 T visas that Congress sets aside for human trafficking victims every year."

Something has gone wrong here; victims of human trafficking are not applying for help that is available to them. Mandatory biometric collection of infants and children under 14 is likely to exacerbate these problems.

The Council of Europe's *Convention on Action against Trafficking in Human Beings* specifically discusses the need to protect the private life of and identity of victims, including victims who are children. Article 11 – Protection of private life — states:

> 1. Each Party shall protect the private life and identity of victims. Personal data regarding them shall be stored and used in conformity with the conditions provided for by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).
> 2. Each Party shall adopt measures to ensure, in particular, that the identity, or details allowing the identification, of a child victim of trafficking are not made publicly known, through the media or by any other means, except, in exceptional circumstances, in order to facilitate the tracing of family members or otherwise secure the well-being and protection of the child."

The DHS proposed biometric collection of infants and children of all ages would be unlikely to comply with CoE's *Convention on Action against Trafficking in Human Beings* because it has not indicated how it proposes to meet the requirements of 1 and 2, above. Biometric identification is sensitive, and the NPRM did not disclose any specifics of what it would do to specifically comply with this convention. Would the data be stored according to the CoE convention? Would there be measures in place to ensure identity details (including biometrics) were kept secured? What are those protective measures?

Rijken and Koster argue that victims of trafficking must be provided with specialized medical care as well as legal aid, and need to be given assistance regarding the "juridical consequences of filing a complaint and testifying against perpetrators." They also discuss in detail the extent to which identity documentation plays a role in acquiring testimony against the perpetrators for state purposes. The authors advocate a "victim centered approach," where the goals of granting robust assistance to victims first and foremost take precedence over the goals of government in identifying victims.[20]

**III. More on the collection of biometrics of children of all ages**

---

[20] Rijken Conny RJJ, Koster D. *A human rights based approach to trafficking in human beings in theory and practice,* May 2008. Available at SSRN: https://ssrn.com/abstract=1135108 or doi: 10.2139/ssrn.1135108

UNICEF and the World Bank in their 2019 report, *Biometrics and Children: A literature review of current technologies*, documented the literature on performance of biometric technologies for children ages 0-18. The evidence indicated that while some biometric technologies may have applicability to older children, biometrics applied to the youngest children (5 and below) are "largely experimental and require more research." The report notes a critical lack of "verifiable performance data on most of the technologies currently in use with children, and the need for more transparency and critical assessment of the impact of population-scale applications." UNICEF has also released guidelines for the use of biometrics and children.[21]

Prior to releasing this NPRM, DHS needed to conduct at a minimum a similar type of evaluative work that UNICEF has completed. There should be a full-fledged framework, developed by all relevant stakeholders, including members of the public, that guides the DHS on this very sensitive topic. The collection of biometrics of children under the age of 14 should not commence unless and until this work is completed.

Beyond the technical considerations regarding the collection of biometrics of children, which are extensive, the ethical considerations were not addressed whatsoever in the NPRM. In the UK, a data ethics advisory service (Biometric Forensics Ethics Group) is providing guidance and support to Home Office projects. It utilizes the data ethics framework[22] developed by the Department for Digital, Culture, Media and Sport.[23] The U.S. needs to catch up here — where is the US government's ethical framework for this NPRM's proposed uses of biometrics in children of all ages? Where is the deliberative, multistakeholder work that would inform this process? Where are the ethical checks and balances that would ensure proper oversight and accountability?

We further note that the proposed rules in the NPRM for the collection of childrens' biometrics younger than 14 is in opposition to the DOJ EOIR system. Unless and until this disparity in ages and processes is addressed, DHS should not be introducing a parallel system with different age requirements. The NPRM states:

> DHS recognizes that removing the age restrictions associated with biometrics collection in DHS regulations, without removing the age restrictions in DOJ EOIR regulations, could create disparate processes for biometric collections in immigration adjudications. Specifically, a child under 14 may be required to

---

[21] *Faces, fingerprints, and feet: Guidance on assessing the value of including biometric technologies in UNICEF-supported programs,* October 2019, UNICEF. https://data.unicef.org/resources/biometrics/.

[22] UK Data Ethics Framework, 2019: https://www.gov.uk/government/publications/data-ethics-framework

[23] UK Department for Digital Culture Media and Sport, https://www.gov.uk/government/organisations/department-for-digital-culture-media-sport

> submit biometrics for an application submitted to USCIS, but the same child would be exempt from biometrics for an application submitted with DOJ EOIR. These disparate authorities could also cause confusion given USCIS collects biometrics at its ASCs for many applications and petitions adjudicated by EOIR. However, DHS and DOJ will continue to be bound by their respective regulations. To the extent that any controversy may arise interpreting DHS and DOJ regulations regarding the removal of age restrictions for biometrics collection, until DOJ removes its age restrictions DHS intends to follow DOJ regulations with respect to age restrictions when collecting biometrics for an application or petition that will be adjudicated by EOIR.

This paragraph in the NPRM is a red flag that the proposed "all ages" system, not having symmetry with the DOJ system, is not ready for deployment. All told, DHS has much more work to do prior to being able to deploy biometric collection and use for people of all ages. It is premature for this proposal to go forward.

As we have discussed, the collection of the biometric data of infants through all age ranges is unprecedented and is not mirrored by the U.S. DOJ EOIR system.

**IV. Conclusion**

There is a fundamental difference between utilizing new technology in an ethical and sustainable way, and utilizing technology such as biometrics on children of all ages, including infants, without a meaningful ethical framework in place to guide those actions and activities. In 2018, WPF's Executive Director spoke before a gathering of international data protection authorities and called for a Nuremberg Code for our digital times, saying:

> The Nuremberg Code was created so as to ensure that humans never repeat the mistakes made in WWII….This code grew from a response to reality, it did not originate as an abstract theory of ethics. Today, we need a new Nuremberg code for digital activities, based in the specific realities of our times, and focused on digital and data ethics.[24]

One place to begin work on establishing a better way forward would be with the Chief Privacy Officer of DHS.

The Chief Privacy Officer (CPO) of DHS has full authority to identify problems in systems and to make sure that DHS components address them. The CPO has primary

---

[24] *Address to the 40th International Conference of Data Protection and Privacy Commissioners*, *Pam Dixon.* World Privacy Forum, October 2018. https://www.worldprivacyforum.org/2018/10/ed-pam-dixon-calls-for-a-nuremberg-code-of-digital-ethics-addresses-40th-international-conference-of-data-protection-and-privacy-commissioners/

responsibility under Section 222 of the Homeland Security Act of 2002, as amended, for privacy policy at DHS. This responsibility includes assuring that the use of technologies sustains and does not erode privacy protections relating to the use, collection, or disclosure of personal information. The CPO has the authority to require DHS employees to comply with policies to ensure that all individuals have suitable privacy protections, regardless of citizenship and immigration status — in compliance with E.O. 13,768 — for personally identifiable information (PII) collected, used, retained, or disseminated by DHS. Pursuant to this responsibility, the law requires that the Fair Information Practices serve as the framework for privacy policy and implementation at DHS.

The Chief Privacy Officer must be granted full authority to review the proposed systems, and to propose changes as needed. Beyond that, the US government needs to begin a serious slate of work regarding a data ethics framework to guide the use of technologies, one which is robust and will address the many difficult issues biometrics collection and use presents, including in children.

Another place to begin work lies in establishing a robust and meaningful multistakeholder process, inclusive of the public, subject to OMB Circular A-119,[25] that would begin work on an ethical framework that could be utilized in considering both this NPRM, and others.

Thank you for your consideration of our comments. Please do not hesitate to contact us with any questions or for additional information.

Respectfully submitted,

Pam Dixon,
Executive Director,
World Privacy Forum

3 Monroe Parkway
Suite P #148
Lake Oswego, OR 97035
www.worldprivacyforum.org

[25] OMB Circular A-119, Office of Management and Budget, The White House. https://obamawhitehouse.archives.gov/omb/circulars_a119