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

Testimony of Pam Dixon to the Port of Seattle Commission regarding the Commission Proposal Regarding Facial Recognition

Port of Seattle Commission
Commission Chambers
Pier 69
2711 Alaskan Way
Seattle, WA 98121

December 10, 2019

Dear Commissioners:

Thank you for the opportunity to comment on biometric policy at this important meeting. Regrettably, we did not learn of the Port of Seattle Commission's earlier meetings regarding biometrics until a week ago. As such, I acknowledge that we are later to the discussion than I would like.

Nevertheless, the World Privacy Forum is pleased to submit comments to the Port of Seattle regarding its biometric policy agenda item at this meeting. WPF is one of the top ten global organizations working on digital identity, including biometrics. I have conducted extensive peer-reviewed field research in biometrics, including on India's Aadhaar biometric system, which is the largest biometric system in the world. Our research regarding India's biometric identity system was published in Nature Springer and was cited twice in India's landmark Aadhaar Supreme Court Ruling of 2018. 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.,* 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/.

All biometric data, including genetic data, rises to the level of high sensitivity. As such, WPF proposes that biometrics be designated as a ***technology of very high concern***, and be subjected to meaningful safety guardrails.

We define biometrics using a modern, technically-aware definition that we developed with leading global biometricians for use in policy settings:

> Biometric data means an individual's physiological, biological or behavioral characteristics that can be used, singly or in combination with each other or with other

identifying data to establish individual identity. These include but are not limited to imagery of iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template (e.g. a faceprint or a minutaie template or voiceprint, etc) can be extracted as well as keystroke patterns or rhythms, gait patterns or rhythms, sleep health or exercise data that contain identifying information.

The US is one of the few countries where biometric technologies have not yet been as pervasively implemented as in other jurisdictions. But it is very unlikely that the US will fully escape the use of biometrics, as seen in airport biometric entry/exit programs, among other biometrics programs.

Because of the significant risks inherent in the uses of the technology, biometrics —including facial recognition— should be classified as a high-risk technology, and procedural safety protections that are well-tested and understood in other high-risk contexts should be adapted for biometrics and put in place as guardrails.

The guardrails we are proposing are similar to those found in existing safety regulations in the US and Europe. We encourage you to consider and adapt these procedures, as they have been discussed by core stakeholders, and have been refined based on many conversations.

Regulatory Safety Structures that Act as Guardrails for Biometric Systems (Facial Recognition)

The protections fall into three key areas: pre- and post-market safety and quality regulations, use controls, and a consumer complaint mechanism.

Pre-and Post Market Safety and Quality Regulations

The following pre and post-market safety regulations for biometrics are derived from the existing legislative models of RoHS, REACH, and the Chemical Safety for the 21st Century Act (updates US Toxic Substances Control Act) as well as the Fair Credit Reporting Act. Finally, the consumer complaint mechanisms at the CFPB and CDC provide the model for the post-market consumer complaint reporting.

- **Classification: Biometrics would be classified as a "technology of very high concern."**

- **Applicable to full supply chain:** The regulations would apply to the full supply chain and to any entity that produces, develops, sells, assembles, distributes, installs, and uses biometric systems.

- **ID risks and reporting requirements**: Biometric entities would be required to identify risks in the technology and document and report those risks to the applicable government body.

- **Testing requirements**: Biometric technologies available for use would be required to be tested and evaluated by NIST for *accuracy* and *bias* on a regular basis, at a minimum, this review would be updated annually.

- **Proven safe prior to launch**: The technology must be proven safe and fit for purpose prior to launch, and must be cleared for market by the appropriate government oversight body. For facial recognition, a non-discrimination analysis would need to be performed.

- **Product labeling**: The biometric product would be labeled for accuracy and for bias. (Facial recognition.)

- **Certification and training requirements would apply.**

- **Ongoing monitoring**: The full supply chain of vendors and implementors must agree to ongoing monitoring and documentation for compliance. Monitoring can be in real time, or near real-time.

- **Benchmarking program metrics**: the stated goals of the biometric installation or program should be tested against benchmarks to factually determine effectiveness and capture hot spots.

Use controls:

Biometric technology is deployed in specific use cases. Some use cases are not objectionable, however, some uses cases are objectionable and pose serious threats of either discriminatory impact or harm. Use case controls derive from the model of the Fair Credit Reporting Act.

- Some use cases of biometrics would not be allowed due to safety considerations, or lack of functionality. For example, body cameras equipped with real-time facial recognition are viewed by biometricians and a majority of law enforcement as a high-risk use case. This particular use case has both legal and technical problems.

- Allowed use cases would have significant definitional controls and procedural requirements. For example, biometrics used in law enforcement investigatory settings would be subject to the procedures set forth at the Federal level. At the state level, the Bureau of Justice Assistance procedures for biometrics use, for example, could be required. https://www.bja.gov/Publications/Face-Recognition-Policy-Development-Template-508-compliant.pdf.

- Voluntary Consensus Standards could be used in conjunction with legislation to establish ongoing multistakeholder evaluation of emerging use cases.

Post-Market Consumer Complaint Reporting:

- Voluntary Consensus Standards could be used in conjunction with legislation to eUsing the adverse event reporting model and the consumer complaint model, biometrics technologies would have a dedicated post-market monitoring mechanism at the federal level.

- Consumers and others would be able to submit complaints to a central structure.

- As with the structure of the existing Consumer Financial Protection Bureau (CFPB) consumer complaints database, complaints would be available for viewing within a matter of a week, and the complaints would be available for download and analysis. This data will provide ongoing insight into problem areas and detailed implementation feedback.

Key Underlying Safety Statutes

RoHS: EU Directive, also implemented in some US states.

- As of July 2019 all RoHS deadlines active; Directive is now applicable to any business that sells electrical or electronic products, equipment, sub-assemblies, cables, components, or spare parts directly to RoHS-directed countries, or sells to resellers, distributors or integrators that in turn sell products to these countries, is impacted if they utilize any of the restricted 10 substances.
- Requires products to be cleared for market prior to launch and meaningful compliance documentation/recordkeeping from all parties in the supply chain, regularly updated information, mandatory compliance labeling.
- **In the US**, California, Colorado, Illinois, Indiana, Minnesota, New Mexico, New York, Rhode Island, and Wisconsin have enacted RoHS-like and e-waste regulations.

REACH: EU Regulation

- Applies to essentially every product manufactured, imported, or sold within the EU.
- REACH regulates chemical substances, particularly those known as Substances of Very High Concern (SVHC). Substances considered carcinogenic, mutagenic, toxic for reproduction, or bioaccumulative fall under SVHC criteria.
- EU manufacturers and importers are required to register all substances produced above a set yearly volume to:
- ID risks associated with the substances they produce
- Demonstrate compliance in mitigating the risks to ECHA
- Establish safe use guidelines for their product so that the use of the substance does not pose a health threat.

Chemical Safety for the 21st Century Act: US, federal

- Requires pre-manufacture notification for new chemical substances prior to manufacture.
- Where risks are found, requires testing by manufacturers, importers, and processors
- Requirements for certification compliance
- Reporting and record keeping requirements
- Requirement that any person manufacturing (including imports), processes, or distributes in commerce a chemical substance or mixture and who obtains information which reasonably supports the conclusion that such substance or mixture presents a substantial risk of injury to health or the environment to immediately inform EPA, except where EPA has been adequately informed of such information.
- The EPA screens all TSCA b§8(e) submissions.

Thank you for your attention to our comments. Biometrics are systems of various technologies, and they are complex. We are deeply invested in how to establish flexible, future-proof (as much as is possible) biometric guardrails.

Thank you for your consideration. We look forward to having further discussions with you and working with the Commission regarding this important topic.

s/

Pam Dixon
Executive Director,
World Privacy Forum