NTIA Privacy Multistakeholder Process
Commercial Facial Recognition Technology
Proposed Principles that Might be Incorporated into a Code of Conduct
(Stakeholder Submitted)
May 16, 2014

I. Individual Control

1. Give consumers appropriate choices about when facial recognition technology and related data is used. (submitted by ACT and NetChoice)

2. Businesses should be allowed to use facial recognition on their property so long as consumers are made aware of its use. (submitted by TechFreedom)

3. In addition to traditional signage, equivalent disclosure should be provided in machine-readable format such that apps like Yelp and Google Maps could tailor businesses displayed to the user according to the user's pre-determined preferences about facial recognition. A simple taxonomy would not raise the implementation challenges that have plagued other efforts at machine-readable privacy disclosures, such as P3P. (submitted by TechFreedom)

4. An entity must receive informed, written, and specific consent from an individual before enrolling him or her in a face recognition database. Enrollment is defined as storage of a faceprint or photograph for the purpose of performing face recognition. (submitted by ACLU)

5. An entity must receive informed, written consent from an individual before using a facial recognition system or faceprint in a manner not covered by existing consent. When an individual consents to the use of a facial recognition system for one purpose, an entity may seek consent from that individual for its use for a secondary purpose. However, the entity may not compel the individual to give that consent. Consent may be withdrawn by the individual at any time. An entity may not use a face recognition system to determine an individual's race, color, religion, sex, national origin, disability or age. (submitted by ACLU)

6. A faceprint or any information derived from the operation of a face recognition system may not be sold or shared except with the informed, written consent of the individual whose information is being sold or shared. (submitted by ACLU)

7. Withdrawal of Consent: A company must make it convenient and accessible for an individual to withdraw use of their FR data, such as through a prominent link that removes consent. (submitted by ACLU)

II. **Transparency**

8. Consumer education is important. (submitted by Internet Association)

9. Businesses should tell people when they are using facial recognition technology. (submitted by ACT)

10. An entity must describe its policies for compliance with these principles including the duration it retains data, how the data is used, how the government might access the data, and the necessary technical specifications to verify accountability. An entity must prominently notify individuals when face recognition is in operation. (submitted by ACLU)

11. Prior to the creation of any faceprint, a commercial entity must provide in (accessible) writing, and with online examples, how the process has been designed and operates. Such disclosures must accurately reflect all its actual intended use(s) (identification, marketing, etc.); how it may or will be connected to other data or digital content services connected to the individual (credit and e-scores, cookies, customer IDs, social media profiles, tracking technologies, data brokers, etc.); what technologies have been or are used in its operation (deep learning/artificial intelligence/semantic analysis, neuro-analysis, etc.); what controls people have over its use, including whether they have ability to determine to approve/disapprove distinct elements. Companies must also identify for approval whether any racial/ethnic data will be generated and how it will be used. (submitted by Center for Digital Democracy)

12. Prior to the introduction of any FR product, a company will conduct tests, using objective measures that are made public, to assess whether its Notice and Consent framework for consumers is meaningful and effective. Such testing should include evaluating FR in the context of how it will be offered using *real market conditions* (assessing, for example, the impact of Notice and Consent when FR applications come bundled into a free product or are referred by a friend on a social network, etc.). (submitted by Center for Digital Democracy)

13. Companies using FR should issue an annual public report that describes its operations; developments; testing results; and other relevant information. (submitted by Center for Digital Democracy)

III. **Respect for Context**

14. Companies using facial recognition technologies that operate anywhere along the spectrum should implement privacy protections for the context of their relationship with consumers. (submitted by Internet Association)

IV. **Security**

15. An entity must keep securely [use reasonable security protections] [use reasonable security measures] [use commercially reasonable measures] information contained in a face recognition system [to protect facial recognition templates] [to protect the images and data they store]. (submitted by ACLU, bracketed language from Marketing Research Association, Interactive Advertising Bureau, and Internet Association)

16. Companies should maintain reasonable retention and disposal practices. (submitted by Internet Association)

17. Storing facial recognition images as proprietary vectors is a form of encryption. (submitted by Marketing Research Association)

V. **Access and Accuracy**

18. An individual must have the right to access, correct, and delete his or her faceprint information. An individual may also access and request correction of information about him or her derived from operation of a face recognition system including information maintained in the audit trail. (submitted by ACLU)

VI. **Focused Collection**

No principles submitted.

VII. **Accountability**

19. An entity must keep securely information contained in a face recognition system. (submitted by ACLU)

VIII. **Factual Findings**

20. Facial recognition is a powerful new technology with the potential to substantially limit anonymity, allow widespread tracking of the public, and facilitate stalking and harassment. (submitted by ACLU)

21. The rise of social networks and other systems that collect and analyze billions of photographs means that the technology exists now to deploy facial recognition widely. This technology will only improve in speed and accuracy in the future. The deployment of facial recognition is likely to be dictated by policy, not technological, limitations. (submitted by ACLU)

22. An individual's face is a durable identifier which only changes gradually over time. Faceprints have long-term utility for identifying individuals – often without their

permission or consent. Studies have shown that faceprints can often identify individuals for more than a decade. (submitted by ACLU)

23. Teens are particularly vulnerable to exploitation because they frequently use new technologies without a full understanding of the long-term consequences of that use. (submitted by ACLU)

IX. **Other**

24. The code of conduct should cover all industries, and should not prevent the use of facial recognition technology to conduct activities that would be permitted through the use of other methods. (submitted by NetChoice)

25. Facial recognition best practices should focus on harmful uses of information (submitted by TechFreedom)

26. For FR services that target or include adolescents 13-17, the company must explain in writing to the teen, and on its website, the intended actual uses of the FR system. Such Notice for teens should be also be objectively tested and made available for public review. For children 12 and under, COPPA applies; however, the same objective testing of Notice for their parent/caregiver is also required. (submitted by Center for Digital Democracy)

27. An entity must treat a faceprint and other information associated with its collection, use, and sharing as the content of communications. Government access to information from a face recognition system that is not covered by the Privacy Act of 1974 should only be authorized pursuant to a warrant issued with probable cause. (submitted by ACLU)

28. When an entity uses a facial recognition system to authenticate the identity of an individual, a reasonable alternative means of authentication must also be offered to the individual. (submitted by ACLU)

29. An entity must take special precautions when using a facial recognition system with teens. In providing notice and obtaining informed consent from a teen, the entity must take account of the teen's age and level of understanding. There must be verifiable parental consent for children under 13. (submitted by ACLU)

30. Signatories to this framework recognize that while voluntary codes of conduct represent an important step in protecting biometric information from exploitation and misuse, it is impossible to protect against the negative effects of this powerful technology fully without government intervention and statutorily created legal protections. (submitted by ACLU)

31. Facial recognition is the use of technology to personally identify an individual by face. (submitted by Marketing Research Association)

32. Harm Based Approach: Where actual harm is found to exist, we encourage all participants of the multistakeholder process to work towards finding effective solutions that address the identified problem and avoid hampering current and future legitimate uses of facial recognition technology. (submitted by Interactive Advertising Bureau)

33. Technology Neutrality: The risks or benefits of facial recognition technology do not depend on the classification of technology or the environments in which it is employed. The code of conduct should apply equally to all applications, both online and offline and should not specify narrow controls and limitations. (submitted by Interactive Advertising Bureau)

34. Public Information Exception: Organizations should be able to process and communicate information where the images are related to matters of public interest, such as news, public affairs, politics, sports, and public figures. (submitted by Interactive Advertising Bureau)