An Ethical Framework for Facial Recognition

Findings of Fact:

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

Principles:

In order to operate an ethical, privacy-protective facial recognition system, an entity must embrace the following principles (which are derived from well-understood fair information practice principles):

- **Collection.** 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.
- **Use.** 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 Consent may be withdrawn by the individual at any time.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.
- **Sharing.** 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.
- **Access.** 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.

- **Misuse.** An entity that maintains publicly accessible data sets linking an individual's identity to a biometric (such as large social networking sites that contain names and photographs) must take all appropriate technical and procedural measures to prevent access to those data sets for the purpose of creating a faceprint database. These measures may include technical degradation of individual images, limiting automated access to relevant databases, and creating contractual obligations binding partners to follow this Ethical Framework.
- **Security.** An entity must keep securely information contained in a face recognition system.
- **Accountability.** An entity must maintain a system which measures compliance with these principles including an audit trail memorializing the collection, use, and sharing of information in a facial recognition system. The audit trail must include a record of date, location, consent verification, and provenance of the faceprint and other data. It must also allow evaluation of the faceprint algorithm for accuracy. This data may also be incorporated in a watermark to ease the ability to audit.
- **Government Access.** 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.
- **Alternatives.** 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.
- **Children and Teens.** 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.
- **Transparency.** 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.

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.