FTC Staff Report:

Facing Facts - Best Practices for Common Uses of Facial Recognition Technologies

NTIA Privacy Multistakeholder Meeting
March 25, 2014

Amanda Koulousias, Attorney
Division of Privacy and Identity Protection
Federal Trade Commission

The views expressed are those of the speaker and not necessarily those of the FTC.

Face Facts: A Forum on Facial Recognition Technology

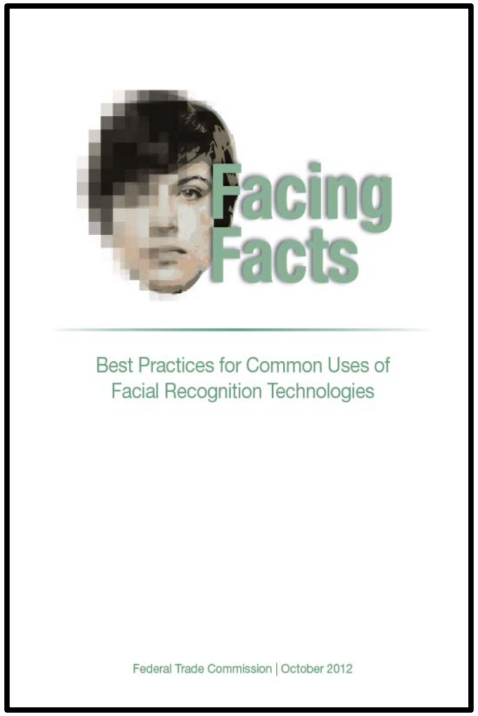
December 8, 2011

- **Panelists discussed a range of technologies**:
  - pure facial detection
  - age and gender recognition
  - emotion recognition
  - facial recognition
- **Major topics included**:
  - Advances in the technology
  - Current and potential future commercial uses
  - Benefits & privacy concerns

Public Comment Period
December 2011 - January 2012

- **Issues for comment included**:
  - Current and future uses
  - Benefits to consumers
  - Privacy and security concerns
  - Best practices for building privacy into products and when and how to provide consumers with notice and choice
- **The FTC received 80 public comments from a variety of stakeholders**

FTC Staff Report: Facing Facts – Best Practices for Common Uses of Facial Recognition Technologies October 2012



Facing Facts

Best Practices for Common Uses of Facial Recognition Technologies

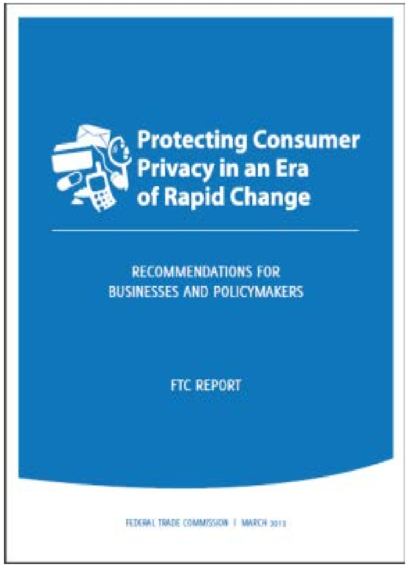
Federal Trade Commission | October 2012

Important Points:

- The report contains recommendations for best practices
    - It is not a template for law enforcement actions or regulations under laws currently enforced by the FTC
- The recommendations build on the workshop and the public comments
- The report uses 3 case studies as an example to discuss best practices

FTC Staff Report: Facing Facts – Best Practices for Common Uses of Facial Recognition Technologies October 2012

- The recommendations describe how companies can implement the principles contained in the FTC's March 2012 Privacy Report:



Protecting Consumer Privacy in an Era of Rapid Change

RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS

FTC REPORT

FEDERAL TRADE COMMISSION | MARCH 2012

- **Privacy by Design**
- **Simplified Consumer Choice**
- **Transparency**

Case Study: Detection or Recognition of Demographic Characteristics in Digital Signs

Privacy by Design:

- Reasonable data security protections to prevent unauthorized access to the images
- No signs in sensitive areas
- Limited data retention

Simplified Choice & Increased Transparency:

- Clear notice to consumers that these signs are in use – before the consumer comes into contact with the sign
- Obtain affirmative express consent before individually identifying consumers through these signs

Case Study: Facial Recognition in Online Social Networks

Privacy by Design:

- Reasonable data security for the database of images & biometric data
- Protections in place to prevent unauthorized scraping of publicly available images in the database
- Appropriate retention and disposal practices

Case Study: Facial Recognition in Online Social Networks (continued)

Simplified Choice and Increased Transparency:

- Clear notice – outside of a privacy policy – when the feature is rolled out

- Offer consumers an easy to find choice not to have biometric data collected and used for facial recognition

- Do not collect or store biometric data of non-users of the service because there is no context in which to provide such non-users with a choice about these practices

Case Study: Facial Recognition in Online Social Networks (continued)

Situations in which affirmative express consent should be obtained:

- Before using a consumer’s image or biometric data in a materially different manner than represented when the company collected the data

- Identifying a user to another user who is not their “friend”

- Recommendation applies beyond social networks:

  - Only identify anonymous images of consumers to someone who could not otherwise identify them if the consumer has affirmatively opted in to such a system

Questions?