THE COMMERCIAL FACIAL RECOGNITION ACT

A COMPROMISE BILL FOR CONSUMER PRIVACY

Courtney Matteson, Nchinda Nchinda, Kiran Wattamwar

FACIAL RECOGNITION TECHNOLOGY (FRT)

FRT is able to identify an individual using algorithms to analyze the unique characteristics of a face in a visual input.

least dangerous privacy concerns

FACIAL DETECTION
Is there a face in this image and where?

FACIAL CHARACTERIZATION
What assumptions can I make about the person in the image (demographics like age, gender, etc.)?

FACIAL VERIFICATION
Is the person using the system who they claim to be?

FACIAL IDENTIFICATION
Who is the person in the image, by name or other personally identifiable information?

most dangerous privacy concerns

FRT IN PRACTICE

The FindFace app can **identify strangers in a crowd with 70%+ accuracy**, pulling data from the Russian social network, Vkontakte for facial identification.

Facial data are **durable identifiers** currently regulated only at the state level by Texas and Illinois with **few other external regulations**.

RISKS

- Images can be **taken from a distance and processed** instantly
- Stalking and harrasment
- Loss of anonymity in public spaces

BENEFITS

- Improve privacy/security of tech
- Prevent theft
- Identify missing children

This act aims to secure consumer safety without stifling innovation

1. TRANSPARENCY Require companies ("covered entities") that collect and attribute biometric and other FRT-enabling data ("facial data") to a specific identified human individual ("data subject") to disclose how they use, store and disclose the data;

2. NOTICE AND CONSENT Require covered entities to provide notice to and obtain consent from subjects prior to enrolling or changing the intended use of the subject's protected facial data, with the exception of periods of internal product development.

3. FAIR USAGE OF DATA Restrict certain uses of FRT that violate consumer privacy expectations by using protected data outside of the context for which it was collected, that discriminate against individuals according to certain classifications.

4. DATA SECURITY Require minimum security and data retention standards to prevent unauthorized persons from accessing protected data or compromising the integrity of the system, and industry, as a whole.