Ads with Eyes Get a Closer Look

by Joseph Lorenzo Hall [1]
October 26, 2012

Facial recognition technology is both increasingly useful and increasingly problematic. The technology is widely available and easy to use. It is being applied to photo tagging, to targeting advertisements in stores, and to computer security and authentication. Facial recognition once required access to large databases of photographs and significant computing power available only to large corporations and governments. Today it is available in free software packages and in the handheld computing devices that millions of us use every day.

This week the Federal Trade Commission released, "Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies [2]," a report aimed at the growing number of companies using the technology. The report is intended to a guidebook for developers on how to better protect consumer privacy as they build new products and services designed around facial recognition technology. Ahead of the FTC report, CDT released its own report [3] on facial recognition that compares how the U.S. and E.U. treat the technology with respect to the law and policy making.

Throughout the report, the FTC cites the comments [4] CDT submitted in December, 2011. We feel that the guidance here from FTC is timely and reflects a measured balance with respect to consumer privacy without impeding the amazing innovation the facial recognition market is developing and deploying.

We echo the FTC in highlighting the importance of protecting the consumer with a three-level, conceptual approach to the use of facial recognition technologies:

- Level 1: Counting: Facial information is detected but not used to tailor advertisements and no information is retained or linked to other sources of data.
- Level 2: Targeting: Facial information is detected and used to tailor advertisements — demographics like age, ethnicity, etc. — and no information is retained or linked to other sources of data.
- Level 3: Identification: Facial information is detected, used to tailor advertisements and also linked to an individual's identity or piece of property.

The privacy concerns escalate moving from level one to level three. We believe technologies at level 1 or 2 should provide consumers with a conspicuous notice that facial recognition technology is in use, but not require an explicit "opt-out" because there is nothing to opt-out of given no link to identity.

Level 2 technologies should be mindful of sensitive populations like small children and turn advertising off or display a privacy policy when a child is looking at the screen. Similarly, we feel that level 3 technologies shouldn't be allowed in places people can't avoid, such as health care facilities and government services facilities. Level 3 technologies should also give consumers the option to opt-out of such collection and that any transfer of facial information should require explicit and informed consent.

To their credit, many businesses are already mindful of privacy issues [5]associated with facial recognition and have taken steps to reduce its impact on consumer privacy.

While these self-regulatory steps are important, industry standards today do not encompass the full range of commercial applications for facial recognition. There is no "one size fits all" solution for the privacy concerns raised by this technology. Moreover, given the numerous other ways to identify and track consumers using biometric information, it's doubtful that any solution targeting facial recognition is even appropriate. Instead, a mix of policy and technical approaches will be needed to give consumers a greater measure of control over how facial recognition is used without unduly

limiting its benefits.

CDT recently presented its own facial recognition paper [3] at the 2012 Amsterdam Privacy Conference discussing the problems posed by facial recognition, the responses from industry in terms of self-regulation, the state of law and policy in both the United States and the European Union, and recommendations that we feel will help the marketing industry better respond to privacy concerns given the increasing use of facial recognition.

- FTC
- Facial Recognition
- Consumer Privacy

Links:
[1] https://cdt.org/personnel/joseph-lorenzo-hall
[2] http://www.ftc.gov/opa/2012/10/facialrecognition.shtm
[3] https://www.cdt.org/files/pdfs/CDT_facial_recog.pdf
[4] https://www.cdt.org/blogs/harley-geiger/612facial-recognition-and-privacy
[5] https://www.cdt.org/blogs/harley-geiger/digital-signage-federation-adopts-privacy-standards