

Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law
Hearing on “What Facial Recognition Technology Means for
Privacy and Civil Liberties”
July 18, 2012

Questions for the Record from U.S. Senator Al Franken
for Ms. Maneesha Mithal

- 1. Is there currently anything in federal law that would require a company to get someone’s consent before that company generates a faceprint for that person?**

I am not aware of any federal laws currently in effect that specifically require a company to obtain an individual’s consent before generating a faceprint for that individual. However, Section 5 of the Federal Trade Commission Act (“FTC Act”) prohibits unfair or deceptive acts or practices. 15 U.S.C. § 45 *et seq.* In certain instances, a company’s generation of an individual’s faceprint without consent may be unfair or deceptive, such that the Federal Trade Commission (“FTC” or “Commission”) could bring an action under the FTC Act. For example, if a company represents to consumers that it will not generate faceprints from the images that consumers provide to the company, and then subsequently begins generating faceprints from the previously provided images without obtaining the consent of those users, this may be deceptive under Section 5. If a company generates a faceprint in a way that causes or is likely to cause substantial injury that is not outweighed by countervailing benefits to consumers or to competition and is not reasonably avoidable by consumers, this would be an unfair practice under Section 5. We would examine these issues on a case-by-case basis.

- 2. Both Facebook and Google are under either final or proposed settlement orders with the Commission that require those companies to protect their customers’ data in particular ways. These orders also subject those companies to 20 years of Commission privacy audits.**

Do these settlement orders cover these companies’ use of facial recognition data like faceprints, and if so, how do they protect that data?

Both the final order in the Google matter, as well as the proposed consent order in the Facebook matter, define the information covered by various provisions of the orders (“covered information”) broadly. The Google order defines covered information as, “information respondent collects from or about an individual...” Similarly, the proposed Facebook consent order defines covered information as, “information from or about an individual consumer...” Because faceprints, as well as the consumer images they are derived from, are “from or about an individual” they fall under the definition of covered information in both orders.

The orders require the companies to protect covered information in a number of ways. For example, it would be a violation of both the Google order and the proposed Facebook order for the companies to misrepresent the extent to which they protect consumers' faceprints. Further, if either company were to have or launch a facial recognition feature without conducting a review to assess and address the privacy risks associated with that feature, this conduct would violate the provision of the orders that require the companies to implement a comprehensive privacy program.

Additionally, the proposed Facebook order requires that the company obtain users' affirmative express consent before sharing information that is restricted by a privacy setting with any third party in a way that materially exceeds that privacy setting. Thus, once the order is finalized, if Facebook did not obtain users' affirmative express consent before implementing a facial recognition feature that overrode users' privacy settings, this conduct would violate the order. A similar prohibition applies in the case of Google.

The FTC can obtain civil penalties of up to \$16,000 per violation per day for violations of final orders.