



POLICY & ACTION FROM CONSUMER REPORTS

January 31, 2012

Federal Trade Commission  
600 Pennsylvania Avenue N.W.  
Room H-113 (Annex P)  
Washington, DC 20580

Submitted via [www.ftc.gov](http://www.ftc.gov)

Comments of Consumers Union on  
*Face Facts: A Forum on Facial Recognition*  
Project Number P115406

Consumers Union,<sup>1</sup> the public policy and advocacy division of *Consumer Reports*®, appreciates the opportunity to provide comment on “*Face Facts: A Forum on Facial Recognition Technology*” -- a public workshop organized by the Federal Trade Commission (FTC) to explore the current and future commercial applications of facial detection and recognition technologies. We thank the FTC for organizing this informative workshop, and for the agency’s increased focus on the potential benefits but also risks surrounding the use of facial detection and recognition software.

The ability to detect and recognize a person’s face in real time in order to instantly provide personalized content has captured our imagination for years. Numerous science fiction movies and novels have explored this possibility, imagining a world where biometric data is used to verify identity, to deliver ads and other personalized content, or even to allow government tracking and monitoring of individuals. In light of today’s rapidly evolving technological environment, however, these scenarios have begun to sound less improbable than ever before. Already, facial detection and recognition technologies have been adopted in a variety of new contexts, ranging from online social networks to digital signs and mobile apps.

While the potential benefits of this technology could be immense, there are also incredible risks that we must both acknowledge and address before we can embrace its widespread use in marketing, advertising, or social networking. The ubiquitous installation of facial recognition devices in malls, supermarkets, schools, doctor’s offices

---

<sup>1</sup> Consumers Union is the public policy and advocacy division of Consumer Reports. Consumers Union works for telecommunications reform, health reform, food and product safety, financial reform, and other consumer issues. Consumer Reports is the world’s largest independent product-testing organization. Using its more than 50 labs, auto test center, and survey research center, the nonprofit rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 8 million subscribers to its magazine, website, and other publications.

and city sidewalks could seriously undermine individual's desire and expectation for anonymity. We will address some of these possible challenges in the comments below.

### **Facial detection v. facial recognition software**

As outlined at the public workshop, *facial detection* software does not identify a specific individual, but only detects the presence of a human face. Such technology may be able (with some degree of accuracy) to determine whether a person is male or female, and their general age range. But it does not connect the face with a specific identity.

*Facial recognition* software, on the other hand, analyzes an unknown human face in order to determine the actual identity of the person. This could be achieved by comparing the unknown face to a database of previously identified faces and finding a "match."

Because facial detection software does not actually connect an individual's face with their identity, it appears to pose fewer privacy risks, as long as companies follow strict standards to ensure individuals' privacy is protected. First of all, the information collected must remain completely anonymous and at no point in time should it be re-identified. The technology should also not attach any persistent identifiers to the data, even if those identifiers do not contain personally identifiable information. Persistent identifiers should never be used to save and later track a specific face, creating a behavioral profile that can be used for further targeting. Again, it does not matter if this profile is associated with an individual's identity or a persistent identifier of some other sort.

Secondly, the software must not retain or transmit the data collected. Any information about an individual human face must be erased immediately after the personalized content is delivered. Under no circumstance should that information be retained and repurposed by the collecting party, nor should it be transmitted to third parties for additional uses.

Finally, companies must develop ways to give individual's clear and transparent notice about the use of the technology, as well as the means to avoid it if it makes them uncomfortable.

Facial recognition, on the other hand, is a much thornier issue, and the potential for mischief is significantly greater. As a result, we believe that any use of facial recognition technology to actually identify an individual should only occur with that individual's express and informed consent.

The potential uses of facial recognition technology raise numerous privacy concerns. For example, companies could develop services that offer to analyze and identify unknown individuals in users' pictures. Using this service, anyone could identify any individual simply by taking their picture on the street. Facebook is currently using a version of this technology in order to suggest name tags on users' photos. The Facebook service only suggests name tags for a user's friends, however, not for the entire Facebook community. We think users should have to opt in to have their face analyzed and categorized using

Facebook's software. In addition, in light of Facebook's 800 million active users who upload around 200 million photos per day, we continue to be concerned that this technology could ultimately allow anyone to search for a person simply by using a photo.

No clear standards currently exist for the use of facial identification software, which could allow industry to simply make up rules as they go along. We believe clearer standards need to be in place to ensure consumers' privacy rights are protected.

### **Vulnerable populations**

Facial detection or recognition software should not be used to target ads to children. Food marketing to children and youth, in particular, has been extremely problematic in light of growing childhood and youth obesity rates. A 2005 study estimates that over 80% of food ads displayed during children's TV shows are for convenience/fast foods and sweets.<sup>2</sup> Young children, however, are often unable to understand the persuasive intent of advertisements.<sup>3</sup> The ads and cartoon characters they see on TV influence the types of foods they ask their parents to purchase, as well as the foods they are willing to eat.<sup>4</sup>

In addition, we also concerned about the targeting of weight loss and muscle building supplements to teens. Many teens struggle with self esteem issues during adolescence and are often unhappy with their bodies, making them particularly susceptible to weight loss and bodybuilding supplement claims.

With the evolution of facial detection programs, manufacturers of sugary soft drinks and cereals, fast food, calorie-laden salty snacks, and weight loss and bodybuilding drugs, among others, would be able to discern when a child or teen walks by a digital billboard and to target him or her in real time with personalized ads. We strongly encourage the FTC to set in place guidelines to prevent such uses of facial detection software.

In addition, facial recognition software should certainly not be deployed to identify children under 13, as this would violate the requirements of the Children's Online Privacy Protection Act if done without express parental consent. We are concerned, however, that because teens receive no heightened protections under COPPA, companies could use facial recognition software to identify teens. This could be problematic, especially where the software could be used to dig up potentially damaging teen pictures that could then be used to harm the individual's career or reputation down the road. We strongly believe that teens should receive heightened privacy protections on the Web as a general rule, but would particularly encourage adequate and stringent standards for use of teen biometric data.

---

<sup>2</sup> Harrison K, Marske AL. "Nutritional Content of Foods Advertised During the Television Programs Children Watch Most" *American Journal of Public Health*, 2005, vol 95, no. 9 , pp. 1568-1574.

<sup>3</sup> Kunkel D. et al. *Psychological Issues in the Increasing Commercialization of Childhood: Report of the APA Task Force on Advertising and Children*. Washington: American Psychological Association, 2004.

<sup>4</sup> CSPI Factsheet, "Food Marketing to Children," available at:  
[http://www.cspinet.org/new/pdf/food\\_marketing\\_to\\_children.pdf](http://www.cspinet.org/new/pdf/food_marketing_to_children.pdf).

## **Providing notice to consumers**

Consumers must be given adequate disclosures vis-à-vis the use of facial detection and facial recognition software. In case of digital ads equipped with facial detection technology, companies should place a prominent notice in the vicinity of the ad, or at the entrance to a mall or supermarket that employs such ads.

Consumers should always be able to expressly opt in when the use of facial recognition technology is involved. The privacy risks surrounding facial recognition software are significant, and many consumers are likely to be uncomfortable with the use of this type of technology. As a result, consumers should get to choose, after full and meaningful disclosure, whether the benefits involved outweigh the risks.

## **Conclusion**

Facial detection and recognition software could offer consumers a number of tangible benefits. At the same time, we cannot ignore the fact that these technologies pose significant privacy risks and seriously threaten consumers' right to anonymity. Moreover, the use of such technologies in a non-transparent manner could cause consumers to lose trust in companies and advertisers. If consumers are "creeped out" by companies' advertising practices, they are not likely to respond favorably to that company's brand.

As a result, before these technologies become common-place in our society, we must ensure we have strong, comprehensive privacy standards in place to ensure that consumer information is protected. It will be much more difficult to develop and enforce strong privacy requirements on the back end, once the technology is already being widely used for marketing and other purposes. It also behooves companies to cultivate consumer trust by being completely open and transparent about their targeting practices.

We urge the FTC to ensure that facial detection and recognition technology is developed and implemented with privacy in mind. We look forward to working with you on this issue. Should you have any questions or concerns, please do not hesitate to contact me at (202) 462-6262.

Sincerely,

Ioana Rusu  
Regulatory Counsel  
Consumers Union

1101 17<sup>th</sup> St. NW  
Washington, DC 20036  
(202) 462-6262 – phone

(202) 265-9548 – fax -  
irusu@consumer.org -