Privacy Rights Clearinghouse

Empowering Consumers. Protecting Privacy.

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

January 31, 2012

Face Facts:
A Forum on Facial Recognition
Project Number P115406

Submitted online via https://ftcpublic.commentworks.com/ftc/facialrecognition/.

Privacy Rights Clearinghouse (PRC) appreciates the opportunity to submit comments regarding the privacy and other consumer-protection implications of facial detection and recognition technologies. We also appreciate the opportunity to have participated in the December 8, 2011, workshop, "Face Facts: A Forum on Facial Recognition."

PRC is a nonprofit consumer privacy organization with a two-part mission: consumer education and advocacy. The organization, which was established in 1992, is based in San Diego, California, and serves consumers nationwide. The PRC has invited individuals' complaints and questions since its inception nearly 20 years ago. (Website: www.privacyrights.org)

We applaud the Federal Trade Commission (FTC) for dedicating resources to and addressing the consumer privacy concerns that are raised by the increased commercial use of facial biometrics technologies. We consider facial detection and recognition technologies -- in particular, facial recognition -- to be among the most critical privacy issues of our time.

As the FTC is clearly aware, it is important for the companies both developing and implementing facial detection and recognition technologies to be transparent and privacy conscious. Individuals must be made fully aware when companies collect their personal information, and they must have opportunities to refuse to participate. It is important that individuals know how their information will be collected, used, protected, and made available to affiliates and third parties. Finally, in a data collection landscape that is largely invisible, consumers must be able to have confidence that businesses will abide by their own policies and industry best practices.

3108 Fifth Avenue, Suite A, San Diego CA 92103
Voice: 619.298.3396 ♦ Fax: 619.298.5681 ♦ www.privacyrights.org

If companies engage in Privacy by Design[1], develop privacy policies that incorporate the full set of Fair Information Principles, and are held accountable to a set of best practices with meaningful enforcement mechanisms, the risks of privacy invasion will be significantly reduced.

Privacy Concerns Surrounding the Adoption of Facial Detection and Recognition Technologies

There are numerous privacy concerns surrounding the adoption of facial detection and recognition technologies. The level of intrusiveness depends largely on how the technology is deployed and the purposes it serves.

Facial Detection

On its face, commercial use of facial detection is less intrusive than that of facial recognition. This is especially true if no individualized data is stored and the software is not used to recognize individuals or tie the data to a specific identity. Some speakers at the FTC workshop even presented ways in which facial detection technology can be used for consumer privacy protection. For instance, it may be used to detect faces and then automatically blur them so as to protect the identity of an individual in a photo or video. It may also be used to generate aggregate data that helps a business better serve its customers.

However, facial detection technology may also be used to analyze a person's face and approximate his or her sex, race, age, and mood (among other characteristics) to attempt to influence or persuade that person rather than to simply better understand the consumer. While some consumers may enjoy the benefits of such extremely targeted marketing, others might find it highly intrusive as well as unduly manipulative. This also gives rise to the question of whether such information is or will be used to engage in discrimination of any sort based on a person's perceived characteristics.

In addition, facial detection technology may be largely invisible to a consumer. Since there is currently no mechanism to ensure accountability for implementing industry best practices, consumers are likely to be unaware when facial detection technology is being used unless prominent signage and other notice mechanisms are deployed.

Finally, if images or templates of a person's face are retained for any length of time, it would not be difficult to envision that a business might be tempted to use that data to identify the consumer later. Therefore, limited data retention is key to preventing more intrusive uses of the data. We further discuss data retention below.

---

[1] Privacy by Design is "an approach to protecting privacy by embedding it into the design specifications of technologies, business practices, and physical infrastructures." Privacy by Design incorporates a set of information management principles, and was developed by Dr. Ann Cavoukian, Information and Privacy Commissioner, Ontario, Canada. See Introduction to PbD, Office of the Information and Privacy Commissioner of Ontario, Canada, http://www.ipc.on.ca/english/Privacy/Introduction-to-PbD (last visited Jan. 31, 2012).

See Ann Cavoukian, Ph.D, *Privacy by Design, The 7 Foundational Principles, Implementation and Mapping of Fair Information Practices*, available at http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf .

Facial Recognition

Facial recognition technology can attempt to identify an individual based on the unique characteristics of his or her face, similar to identification based on one's unique fingerprint, palm print, or iris markings. At least one workshop panelist touted the potential for beneficial uses of facial recognition technology (e.g. for use in natural disasters and to identify missing and exploited children).

While there are certainly positive and innovative uses for facial recognition technology that some consumers may affirmatively choose (opt in), there are also numerous ways it can be exploited. This is especially true if businesses creating or deploying the technology do not fully adopt Privacy by Design.

One of our major concerns is that there are no safeguards or tangible incentives in place to ensure that businesses are fully transparent and allow consumers a meaningful opt-in choice to such data collection and use. Furthermore, there is no way to ensure that companies are minimizing the data they collect and store; that they are collecting, storing, and disposing of the data securely; or that the data is being deleted and is not retained for an indefinite period of time.

There is also the possibility that a company would use data for purposes other than those for which it was initially collected. Vast amounts of information exist both online and offline that could be aggregated and combined with face prints to create even more detailed profiles on individuals than already exist. Even if a company were to adopt best practices in its own operations, virtually nothing prevents the company from transmitting the data to third parties that may not have good intentions or sufficient privacy policies and practices in place. Further, nothing prevents the company from changing its privacy policy and practices later.

Children, People with Disabilities, and Non-English Speakers Should be Taken into Consideration when Deploying Facial Detection or Recognition Technologies.

Children under the age of 13 should never be the target of marketing campaigns that use facial recognition or detection technology. Use of such technology should be prohibited in any areas that are specifically geared toward children, and this must be strictly enforceable. In the event that a child's data is inadvertently collected, it must be promptly deleted. There should be no workaround available for a company to collect and retain a child's data to then use it when the child is at the correct age.

In the interest of being transparent, companies must also provide meaningful notice and choice in alternative forms so they are understood by all relevant populations. This means that those with disabilities such as a visual or hearing impairment, as well as those who do not speak English, would need to receive appropriate forms of notice and choice.

Facial Detection and Recognition Technologies Should Be Prohibited in Certain Settings

Certain settings, especially those in which children typically congregate or individuals engage in sensitive activities, should be free of digital signage. The World Privacy Forum's Digital Signage Privacy Principles, which PRC signed on to and supports, lay out certain situations in which the

use of digital signage must be prohibited. Among these are places geared towards children; locker rooms, changing rooms and restrooms; or health-related facilities including: pharmacies, areas where over-the-counter drugs are sold, gyms, and health food stores.[2]

Best Practices for Providing Consumers with Notice and Choice

As facial detection and recognition technologies become more widely used and implemented, it is crucial that businesses are completely transparent when communicating their data practices. Currently, consumers are largely unaware of the use of such technology and the potential privacy implications.

A key concern is that facial recognition and detection devices can be virtually invisible to consumers. In addition, even if the devices are visible, it can be difficult to determine why or how they are being used. For example, how does a consumer know that what he or she thinks is a security camera is really performing a facial detection/recognition function?

Consumers must be clearly notified that the technology is in use at or near a commercial establishment they visit. They also must receive real-time disclosures and privacy policies that are clear and readable, state the purpose of the technology, and offer a viable choice. We firmly believe that notice must move beyond the traditional privacy policies linked to a website, and become more consumer-friendly. Companies should engage the consumer and inform him or her rather than masking the technology and its uses.

If a business uses such technology, it should clearly label both the device being used and the physical area in which a person's image or data may be collected. In addition to clear labeling, we believe that businesses should seek to engage the consumer in a manner that educates them on the privacy policy and is easier than simply providing a link to a website privacy policy.

One possibility would be to prominently post a QR code (or similar concept) at all entrances, digital signs, and point-of-sale areas that a consumer can engage with using a personal device like a smartphone. Using a QR code[3] is just an example to illustrate that there are alternative ways to raise public awareness of such technologies and a business' privacy policy. With proper incentive, the innovators who integrate facial detection and recognition technologies into marketing strategy can surely develop effective and consumer-friendly methods of providing transparent notice.

Sufficient notice is meaningless to consumers without valid choice. This may be opt-out for facial detection with privacy protections built in, but must be opt-in for facial recognition. However, in either situation, the notion that an individual who is uncomfortable with such technology has one option — to avoid the place or area that utilizes the technology — does not signify meaningful choice. Our primary disagreement with the Digital Signage Federation's

---

[2] *See* World Privacy Forum, Digital Signage Privacy Principles: Critical policies and practices for digital signage networks, Feb. 25, 2010 [hereinafter WPF Principles], *available at* http://www.worldprivacyforum.org/pdf/DigitalSignage-principlesfs.pdf

[3] Coupled with brief explanatory text such as "Facial detection technology in use. Learn more here…".

privacy standards is that they accept this option as a viable choice mechanism.[4]

Consumers must be presented with alternatives. These could be as simple as being able to press a button that assures their information or image will not be used or collected, or providing kiosks within the establishment where individuals can opt in. Ideally, consumers should have granular control to engage as much or little with the business and its use of the technology as they feel comfortable (based on clear disclosure and notice).

In the FTC workshop, Joseph Atick raised the notion of a face print being considered personally identifiable information owned by the individual. We believe this concept is worth exploring as a way for consumers to be able to dictate the exact terms under which their face prints are used, retained, or transferred. As long as there were an audit mechanism, the actual ownership interest were nontransferable, and there were precautions in place to keep consumers from being deceived, this idea shows a novel and potentially workable approach to notice and choice.

Notice and Choice are Important, but Businesses Developing and Deploying Facial Detection and Recognition Technology Must Implement Privacy Policies Based on a Full Set of Fair Information Principles and Be Subject to Enforcement

When PRC evaluates a business' privacy policy, we look for ways in which the business implements a full set of Fair Information Principles, or FIPs. These are the principles of Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, and Accountability.[5] Unfortunately, FIPs are often truncated to simple notice and choice. While notice and choice are important, used alone they are insufficient to address consumer privacy concerns and provide sufficient control over the use of one's personal information.

For instance, with pure facial detection technology, it may not be as realistic to provide consumers with the explicit consent mechanisms that must be used with facial recognition. Therefore the device and/ or software must have privacy and security safeguards built in. The company using the technology must also engage in data minimization by limiting collection, only collecting as much information as is needed for the specified purpose, and putting a data retention policy in place. We support a data retention limit of 14 days, as recommended by the World Privacy Forum.[6] The data retention limit recommended by the Digital Signage Federation, in contrast, is 30 days.[7]

---

[4] *See* Digital Signage Federation, *Digital Signage Privacy Standards*, Feb. 2011, at 7 [hereinafter DSF Standards], *available at* http://digitalsignagefederation.org/Resources/Documents/Articles%20and%20Whitepapers/DSF%20Digital%20Signage%20Privacy%20Standards%2002-2011%20%283%29.pdf.

[5] *See e.g.* Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

[6] *See* WPF Principles, *supra* note 2.

[7] *See* DSF Standards, *supra* note 4, at 8.

It is necessary for the industry to have uniform standards to which companies are held accountable. In developing the official standards and best practices, we recommend engaging the participation of consumers or consumer representatives. However, setting an industry standard for consumer privacy protection is only half of the equation. Even if the industry develops a robust set of best practices and attempts to engage in self-regulation, the principle of accountability remains a major concern.

We fear that consumer privacy concerns will not be adequately addressed if businesses are not held accountable at a minimum to government agencies like the FTC or state Attorneys General for their practices. Businesses using facial detection and recognition technologies must also be subject to benchmarking and third-party audits. Without such mechanisms to ensure accountability, it is likely that many bad or careless actors would go unnoticed.

Due to the largely invisible nature of this technology and the data handling practices that surround it, individuals may be ill-equipped to identify and report noncompliance. As an organization that receives privacy inquiries from individuals on a daily basis, we notice that individuals often feel as though their privacy is being violated but cannot articulate exactly why or how.[8] The sectoral legal landscape surrounding privacy in the United States is difficult enough for consumers to navigate without making it the consumer's responsibility to ensure that companies are complying with a loose set of voluntary industry best practices. We encourage the FTC to investigate ways in which the facial detection and recognition industry may be held accountable to consumers and subject to enforcement.

Developing and Deploying Facial Detection and Recognition Technologies in a Way That Protects Consumer Privacy

It is very important that companies developing and using facial recognition and detection technologies are aware of and implement the concept of Privacy by Design far before the technology is implemented in the marketplace. Companies that use and develop such technologies should have a privacy professional involved in both the development and roll-out processes, and also available for consumers to contact when the technologies are in use.

As mentioned above, companies should create and carry out a privacy policy based on a complete set of FIPs. In particular, companies should focus on using data only for limited and specified purposes, retaining data and images for minimal amounts of time, and implementing sound security measures.

For facial detection technology, there should be no way that data collected can then be

---

[8] For example of further study on this concept, see KnowPrivacy, a study finding that users are concerned about online data collection and want greater control over their personal information, users lack awareness, and users don't know to whom to complain. Joshua Gomez, Travis Pinnick, and Ashkan Soltani, *KnowPrivacy*, June 1, 2009, http://knowprivacy.org/.

The Privacy Rights Clearinghouse launched an online Complaint Center in January 2012 that was designed with the results of the KnowPrivacy study in mind. See Privacy Rights Clearinghouse, *A New Year for Privacy: The PRC Launches Online Complaint Center*, Jan. 3, 2012, http://www.privacyrights.org/new-year-for-privacy-prc-launches-online-complaint-center-2012 for more information.

repurposed in the future to identify individuals. From the presentations at the workshop, it appears that Intel's Aim Suite software does a good job of ensuring individual images are not retained.

For facial recognition technology, any consumer participation must be completely opt-in. The Ontario Gaming Commission example presented at the FTC workshop is a good case study.[9] If companies are given incentives to implement FIPs-based privacy protections from the point of inception to the technology's implementation and beyond, both consumers and industry will benefit.[10]

Concluding Remarks

The PRC lauds the FTC's interest in examining the consumer protection and policy implications of facial detection and recognition technologies, both at its December 2011 workshop and this Comments opportunity. We look forward to further opportunities to address this issue with the FTC.

Sincerely,

Beth Givens, Director
Privacy Rights Clearinghouse
3108 5th Ave. Suite A
San Diego, CA 92103
www.privacyrights.org

[9] Information and Privacy Commissioner, Ontario Canada and Ontario Lottery and Gaming Corporation, *Privacy-Protective Facial Recognition: Biometric Encryption Proof of Concept*, Nov. 12, 2010, *available at* http://www.ipc.on.ca/images/Resources/pbd-olg-facial-recog.pdf.

[10] *See e.g.* Nicole Ozer, *Privacy & Free Speech: It's Good for Business*, ACLU of Northern California, Feb. 2009, *available at* http://www.aclunc.org/docs/technology/privacy_and_free_speech_it's_good_for_business.pdf.