Software & Information
Industry Association
1090 Vermont Ave NW Sixth Floor
Washington, DC 20005-4095

January 31, 2011

The Honorable Donald S. Clark
Secretary
Federal Trade Commission
Room H-113 (Annex E)
600 Pennsylvania A venue
NW Washington, DC 20580

Re: Face Facts: A Forum on Facial Recognition -- Project Number P115406

Dear Secretary Clark,

Thank you for the opportunity to comment on the important privacy policy issues raised by developments in facial recognition technology. The Software & Information Industry Association (SIIA) appreciates the Federal Trade Commission's efforts to explore the uses and challenges presented by this still evolving technology through its public workshop in December and this follow-up comment period.[1] We are pleased to be able to contribute to the Commission's effort to map out an approach for making sure that the public is able to benefit from the further development and deployment of these innovative techniques while still preserving privacy.

As the principal trade association of the software and digital information industry, the more than 500 members of SIIA develop and market software and electronic content for business, education and consumers. SIIA's members are software companies, e-businesses, and information service companies, as well as many electronic commerce companies. As leaders in the global market for innovative software and information products and services, our membership consists of some of the largest and oldest technology enterprises in the world, as well as many smaller and newer companies. For nearly two decades, SIIA has worked with policymakers at the Federal and state levels in the United States, and around the world, to examine the implications and operations of privacy and related laws. Some of our members are involved in the development and deployment of facial recognition technology.

[1] See Federal Trade Commission, FTC Seeks Public Comments on Facial Recognition Technology, December 23, 2011 at http://ftc.gov/opa/2011/12/facefacts.shtm

Tel: +1.202.289.7442
Fax: +1.202.289.7097
www.siia.net

General Comments

SIIA urges the Commission to recognize that it has at hand a workable general framework for evaluating and considering the privacy implications of facial recognition technology. This framework was set out in its draft privacy report.[2] An essential aspect of this framework is that the level of effort to provide privacy protection in a particular socio-technical setting should be proportional to the privacy risks involved. In short, privacy is contextual.

This framework lends itself to the case of facial recognition technology. One key fact about this technology is that it is used in a wide variety of socio-technical contexts: preventing ID theft, pursuing terrorists, allowing tagging of online photographs, detecting fraudulent transactions, providing digital signage in shopping malls. While a similar technology is used in each of these contexts, the meaning, purpose, benefits and risks of the use of this technology vary greatly.

The use of the same technology in different contexts does not imply that a similar set of detailed privacy rules should be used in each of the contexts. There need to be high level privacy principles, which the Commission has proposed in its report, that relate to the need for notice and choice, access and correction and so forth. And specific applications of these principles have to be developed for special contexts. Medical information is subject to specific privacy requirements under the Health Insurance Portability and Accountability Act of 1996. Financial information is regulated by the Fair Credit Reporting Act and the Gramm Leach Bliley Act. In addition, there might need to be specific codes of conduct developed for contexts such as mobile applications or mobile payments.

One of our very general comments is that there is no need to develop specialized privacy principles for facial recognition or facial detection technologies. Specific uses of these technologies such as for digital signage purposes in public commercial spaces might require specially tailored principles that relate to the challenges and opportunities of these uses. But it is the uses in these specific contexts that generate the need for specialized principles, not the technology itself. Privacy is context-dependent, not technology-specific.

[2] *Protecting Consumer Privacy in an Era of Rapid Change, A Proposed Framework for Businesses and Policymakers*, Preliminary FTC Staff Report (December 2010).

The idea of privacy regulation for specific technologies was the motivating force behind some attempts, such as those in which the European Union was involved, to develop privacy rules and best practices for RFID technology. RFID is the name for a family of technologies that involve the transmission of information across short distances from a transmitter embedded in a variety of objects to a receiver that can link the information to a larger public or private data communication, storage and processing system. But the technology itself is used in many different settings from supply-chain management to payment systems. No single set of specific norms apply to all these settings. For instance, the idea of on-premises notice that the technology is being used makes less sense in the case of a payment application, where the only function is to get payment information into the traditional payment system, than it does in the case of a consumer item that might have an active RFID chip embedded in it.

SIIA cautions that movement in the direction of privacy best practices or rules for facial recognition as such risks making the same mistake that was made in the case of RFID.

The second general point to be derived from the Commission's privacy report is the proposal to treat certain activities as commonly accepted business practices "for which companies should not be required to seek consent once the consumer elects to use the product or service in question."[3] One example was internal operations of a web site. Another was fraud prevention. As discussed below, some uses of facial recognition or facial detection technology should be treated as falling into this category of commonly accepted business practices.

The third general point is that there is a difference between technologies that attempt to analyze physical characteristics to determine a person's gender and approximate age and technologies that attempt to relate a visual image to a specific person. This distinction can be marked with a linguistic distinction between "facial detection" and "facial recognition." This distinction is important in that the privacy issues raised by technologies that are interested only in determining gender and estimating age differ from the privacy issues that arise when a specific person can be identified. The discussion at the Commission's workshop in December clearly reflected the importance of this distinction. In the comments below, we illustrate how the difference in the context of the use of the technology makes a difference for the privacy regime that is appropriate.

---

[3] *Protecting Consumer Privacy in an Era of Rapid Change, A Proposed Framework for Businesses and Policymakers*, Preliminary FTC Staff Report (December 2010).

Digital Signage

Digital signage in its current form is a variety of facial detection. Technology used in a digital signage application calculates the probability that a visual image is that of a person of a particular age and gender. In its current implementation in private retail stores and public malls, the technology then enables the serving of a relevant ad or discount coupon.

Because it involves electronic and computer analysis of a person's visual appearance, this use of facial detection technology raises privacy issues. In response, the industry has developed self-regulatory proposals.[4] In addition, civil society has developed an additional set of privacy proposals.[5]

At this stage in the use of the technology, however, it is hard to identify substantial privacy risks. As law professor and privacy expert Daniel Solove said at the Commission's workshop, where an automatic device estimates age and sex and hands you a coupon based on that, is that any different from a person doing the same? The person is not identified. Rather, some characteristics are electronically ascertained and this results in a targeted marketing response. The person needs to be informed that the technology is at work, but the need to provide control over the use of the technology is limited, since the privacy risk is so small.

As the use of the information increases, the need for additional privacy protections might increase. For instance, if face print information is retained, this creates a reasonable possibility of identification, even if it is actually used only in an aggregated way to determine the demographics of people who passed by or paused at a store. In this case there might need to be some privacy protections beyond notice.

The privacy risks increase if this face print information is conjoined with use of loyalty cards that contain individually identifiable information, such as that person's name, address, age, and e-mail. Privacy protections might need to scale up as privacy risks increase.

Online Facial Recognition

---

[4] See POPAI, Code of Conduct, at http://www.popai.com/docs/DS/2010dscc.pdf, and Digital Signage Federation Privacy Standards, at www.DigitalSignageFederation.org

[5] See Center for Democracy and Technology, A Framework for Digital Signage Privacy, at https://www.cdt.org/report/framework-digital-signage-privacy and World Privacy Forum, Digital Signage Principles http://www.worldprivacyforum.org/pdf/DigitalSignage-principlesfs.pdf

Social networks are using online facial recognition techniques to allow their members to tag each other's photos. When a photo is uploaded to the site, the technology suggests the name of a friend for tagging, which the user is free to accept or reject. Tagging is already within the capacity of social network users. The facial recognition technology just makes it easier. The privacy risk is that this greater ease of tagging would expose data subjects to more tags than they would like. This risk is clearly different from the privacy risks involved in the use of digital signage, where identification is not possible. For this reason, it is important to ensure that the use of the technology is under the control of the data subject, who can opt-in or opt-out of its use.

Further consent and additional privacy controls might be needed if online repositories of photographs are used to identify individuals more broadly. This might happen, for instance, if a digital signage device transmits images to an online company that compares the images to a reference photo in its files so as to identify the individual and perhaps provide a report of his interests, tastes and preference. Since social networking sites do not allow this kind of activity, the privacy controls they have in place seem adequate to the risks involved.

Conclusion

SIIA welcomes the Commission's workshop and discussion of the privacy implications of this new technology and endorses the distinction made in these discussions between facial recognition and facial detection. We urge the Commission to approach this issue with the type of framework that it outlined in its draft privacy report. In particular, we think the general principles of fair information practices need to be implemented in the specific context in which facial recognition or facial detection technology is actually used. Finally, we urge the Commission not to adopt a one-size-fits all approach to the technology itself, but to welcome the appropriate implementation of the principles based not solely on the technology in use but on the purpose and meaning of the context in which it is used.

If you have any questions about these comments do not hesitate to contact me or Mark MacCarthy, Vice President for Public Policy at mmaccarthy@siia.net.

Sincerely yours,

Ken Wasch
President