



January 31, 2012

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

On behalf of the Security Industry Association (SIA), I would like to thank you for the opportunity to comment on the FTC's workshop, "Face Facts," A Forum on Facial Recognition, Project No. P115406 held on December 8, 2011. SIA represents more than 400 manufacturers, integrators, dealers, and specifiers of electronic physical security solutions. Facial recognition technology can be used within security systems and therefore SIA members have a direct interest in this proceeding.

The benefits of using facial recognition in a commercial setting are many. For example, facial recognition technology can be an effective tool in promoting public safety. Facial recognition can screen for known threats and automatically alert facility staff or public safety officers. The technology could also provide after-incident forensic analysis that would assist law enforcement, and biometric identification can be used to raise the level of security in applications like access control. It could also allow small businesses to track coarse retail demographics such as gender and age without recognizing particular individuals. And facial recognition technologies are used every day in consumer applications such as digital photography and video to improve image quality.

The FTC workshop addressed a number of important topics that will impact the use of this technology within security systems and other applications. For instance, the workshop addressed the issue of whether facial recognition technology always enables personal identification. In our view - whether the technology collects personal information or not - appropriate notification as to what is being collected is currently considered "best practice" in the industry and that practice should continue.

SIA urges the Commission to recognize a distinction between facial detection and facial recognition or identification. As you know, facial detection describes technologies that can detect the presence of a human face (such as its applications to allow you to take better pictures) or identify certain demographic characteristics of a face. This abstract information is stored in aggregate and without retaining the captured images or identifying the individuals. This is

in contrast to facial recognition applications that “match a face with a name.” Second, SIA believes that consumers should have appropriate notice and the ability to “opt-in” to the use of facial recognition that is linked to personal identification. This opt-in could facilitate rapid service processes which require personal identification (such as airline check-in) and its use in high security access control application where access is tied to an enrolled biometric identifier. Particularly in public applications, consumers should always have notice and the option to opt-out by using alternative methods of identification.

Further, privacy controls should be adjusted for the duration of any image retention by an application. For example, an application that catalogs the image of every person who enters a given store and retains that information indefinitely creates a requirement for explicit disclosure. On the other hand, an application that does not store images and only extract demographic data, which is then kept in aggregate, may require fewer privacy controls.

SIA is proud of its members’ leadership in the area of enabling privacy-protecting enhancements within security systems. In 2011, SIA members adopted a “Privacy Framework” that describes certain principles and serves as a guide for the government and industry in striking the right balance between privacy and security. The document is scheduled for review but the current SIA Privacy Framework can be found on the SIA website (<http://goo.gl/TK3kB>).

Thank you for the opportunity to provide comments on this important proceeding. SIA is prepared to work with you as you continue your examination of facial recognition technology. Many SIA members participate in the use and development of software, hardware and other applications relevant to facial recognition and would appreciate being involved with any policy or regulation development.

Sincerely,


Don Erickson
Chief Executive Officer
Security Industry Association