Face Detection & Face Recognition Consumer Applications

Recommendations for Responsible Use

Face detection and face recognition technologies have begun to appear in many consumer and commercial applications such as digital signage and social media. The subject has recently attracted the attention of the Federal Trade Commission, which conducted a day-long workshop in Washington, DC on December 8, 2011, to examine the implications of these technologies to consumer privacy.

Many of these new applications of face technologies can be positive and beneficial to the consumer, but IBIA strongly believes that they must be deployed with utmost sensitivity to the privacy of the consumer and the general public. Since its inception in 1998, IBIA has been recommending responsible use of biometric technologies. IBIA hereby reiterates, in a form adapted to these new applications, its responsible-use guidelines around face detection and recognition, which originally were developed to deal with privacy concerns in CCTV and video surveillance context.

The recommendations below were presented at the FTC Face Facts Workshop.

Foundation

IBIA's recommendations are anchored on the principle that, while a photograph is not a biometric, a faceprint (which is the unique digital code derived from a photograph and which can be matched against a database of known faceprints to establish identity) *is* a biometric and should be considered as Personally Identifiable Information (PII) when stored in association with any other identity meta data. In this elevated status, a faceprint should enjoy all the security and privacy protections bestowed upon other PIIs.

Furthermore, IBIA believes a faceprint is unequivocally owned by the person's identity from which it was generated, and, as such, it may be subject to additional protections arising from ownership rights.

Best Practice Recommendations

With this as our guiding principle, the potential privacy issues raised by face technologies can be addressed by adopting the following best practices:

(1) Memory-less Face Detection Applications — These applications do not extract, store or utilize faceprints; they simply detect the presence of a human face. They may also detect a person's line of gaze, gender and approximate age. For example, they use this information to custom-tailor an advertisement on a digital sign to the appropriate viewing demographic or to aggregate information in order to measure the effectiveness of an advertisement in attracting attention.

Since these applications do not generate or store faceprints, IBIA does not see any implications to privacy. That said, we believe that the digital signage industry should be encouraged to implement effective consumer notice, allow for passive consent, and should exercise restraint in the deployment of these applications by carefully controlling their locus and limiting their pervasiveness.

(2) Face Detection Applications with Memory: Tracking — In this case, IBIA believes the generation and temporary storage of faceprints is required in order to link a person across multiple encounters (tracking). As such, we believe consent needs to be more than just passive in this class of applications. What is at stake is the exploitation of a stored faceprint, even if it is stored temporarily for a few minutes or hours.

While developers of these applications may argue that the faceprints are not identified in the traditional sense of being associated with identifying metadata, such as a name or a telephone number, IBIA believes they are associated with certain metadata that could be privacy invading, such as the location and time of the encounter of the particular identity.

While the standard of protection for this type of faceprint is less than an identity-tagged faceprint, it is still used in a context that could invade privacy, and is a small step away from a full-fledged exploitation of identity-tagged faceprints.

In essence, the storage of a faceprint with such metadata can serve to track an individual, and hence, can serve as an invasion of privacy of movement. It is similar to location service applications or GPS on cell phones, which are turned off by default and are only activated through active consent. IBIA believes something similar needs to be done here to address potential concerns. For example, developers should build mechanisms that allow the consumer to give his or her active consent before being tracked. This could be accomplished by giving them incentives, such as special offers or coupons whenever they participate in a tracking experience within a shop or store.

(3) Full-fledged Face Recognition — These applications require the use of faceprints in two ways. First, they require the long term or permanent storage of faceprints in databases along with metadata containing the identity ("identified gallery") as well as the real-time generation of faceprints of unknown individuals ("probe"), which are matched against the gallery to determine their identity.

In this case, an identity-tagged faceprint should not be added to a gallery without active consumer consent. This is the same principle that IBIA proposed for law enforcement and security applications when CCTV surveillance raised privacy concerns. In that context, we recommended that faceprints not be added to galleries without warrant or documentation of probable cause.

In addition, a faceprint generated from a live image (probe faceprint) must be deleted as soon as feasible after it is determined that it does not match any gallery faceprint. This is IBIA's "no match no memory" principle.

Of course, these applications should not be exempt from explicit and appropriate notice wherever they are deployed.

Privacy-by-Design: Preventing the Harvesting of Face Images

IBIA believes that elevating the standards of privacy-by-design as a methodology to be adopted by the various industries concerned is worthwhile since there are many elements around the new applications of face detection and face recognition that will be difficult to control or regulate at a detailed level. For example, one key area of concern is the process of developing large scale identity-tagged databases by harvesting images from the web. The problem is that once a consumer has posted his or her photograph on a website, there is no recourse or opportunity for consent—someone can download the face image and from it develop the faceprint necessary to perform the recognition.

While this is not a serious threat if it remains on a small scale, the threat becomes more invasive if images can be accumulated automatically into massive databases. Unfortunately, this is now feasible through the use of web-crawlers. This aspect of the problem was addressed in another recent IBIA white paper (*Face Recognition in the Era of the Cloud and Social Media: Is it Time to Hit the Panic Button?*, available from IBIA website, www.ibia.org).

Protecting against building identity databases by harvesting the web requires the implementation of technical measures by those who control the repositories of social media images and the search engine companies. For example, such harvesting can be prevented if the image servers block all web-crawlers that do not originate from search engine entities that have previously agreed to a declared privacy policy. Such a policy would include a commitment not to extract faceprints from these images or not to make them available for general search.

This technical measure can be built into the web servers and is an excellent example of privacy by design. IBIA recommends the adoption of this and other similar measures that aim at assuring the public that their privacy will be maintained as new applications of powerful technologies are adopted and deployed on a mass scale.

Prepared by Dr. Joseph J. Atick.