Face Facts: A Forum on Facial Recognition, Project No. P115406

January 29, 2012

Pursuant to the invitation by the Federal Trade Commission (FTC) to comment on issues raised at its December 8, 2011 workshop entitled **Face Facts: A Forum on Facial Recognition, Project No. P115406**, the International Biometrics & Identification Association (IBIA) is pleased to submit the following responses to the specific questions posed by the FTC.

IBIA is a non-profit 501(c)(6) trade association with offices in Washington, DC at 919 18th Street, NW, Suite 901, Washington, DC 20006.

- *What are the current and future commercial uses of these technologies?*

  Face finding and face recognition applications have been finding increased acceptance and adoption within commercial applications over the last five years.

  For face finding, the applications include digital signage and human machine interface applications where the detection of a human face and its location is important for appropriately positioning advertising and messaging content. In many cases, these applications also determine the gender and the approximate age of the viewer as well as their direction of gaze.

  For face recognition, the applications include information security applications where the face is used as the password or PIN to conveniently unlock a computer or a smart phone.

  It is also used in closed circuit television (CCTV) in commercial retail establishments, financial institutions and in casinos either for spotting undesirable individuals (such as shoplifters, known card counters or those who had signed a self exclusion notice at the casino) or VIPs.

  More recently, face detection and recognition technology has found numerous applications within the context of social media and consumer photo management software, mostly for automatically tagging faces of friends and family.

- *How can consumers benefit from the use of these technologies?*

  These applications mostly give a dimension of convenience for the consumer. For face recognition, it can enhance the security of their computers and smart devices through

their face without having to remember a myriad of passwords and PINs. Face recognition can also help the consumer organize and search the massive amount of photographs that they are accumulating on social media sites or on their computers.

- *What are the privacy and security concerns surrounding the adoption of these technologies, and how do they vary depending on how the technologies are implemented?*

  The presence of large numbers of face images on social media sites creates some potential for privacy abuse. For example, it opens the door to applications that use the repository of tagged face images along with face recognition technology to identify people surreptitiously in the street without their consent, thus potentially piercing the veil of anonymity that we continue to enjoy today.

  It is IBIA's recommendation that face recognition technology in the commercial space should never be implemented without consumer awareness and consent, requirements that would have the important effects of imposing serious constraints on the design of these applications and encouraging the implementation of "privacy by design".

- *Are there special considerations that should be given for the use of these technologies on or by populations that may be particularly vulnerable, such as children?*

  Responsible use should be applicable to all demographics and age groups.

- *What are best practices for providing consumers with notice and choice regarding the use of these technologies?*

  The operative word here is **consent.** The consumers should give their prior consent, which could be passive or active.

  Face detection: passive consent is sufficient and can be achieved by placing clear signage that explains where face detection is being implemented in a public place for marketing purposes. This assumes that the consumer has choice in order to avoid these places (see next response).

  Face recognition: passive consent is **NOT** enough; active consent should be required. As explained in IBIA's position paper on the subject, face recognition involves the exploitation of a faceprint in order to perform the matching and recognition. Our position is that a faceprint belongs to the identity from which it was generated and, therefore, cannot be used by anyone without explicit consent and approval (see Face Detection & Face Recognition in Consumer Applications: Recommendations for Responsible Use, December 2011, Joseph J. Atick, Ph.D., Vice Chairman of IBIA). Thus,

the consumer has to consent in order to allow their face photograph to be converted into a faceprint and added into the database of a face recognition application. The consent should be specific to a given application only.

- *Are there situations where notice and choice are not necessary? By contrast, are there contexts or places where these technologies should not be deployed, even with notice and choice?*

  No. IBIA believes notice and choice should always be required.

  Yes, there are contexts and places where face detection and face recognition technologies should not be deployed. For face recognition, an example would be where people's expectation of privacy are heightened, such as in bathrooms or changing rooms and lockers. Other critical places may include pharmacies and healthcare establishments. In addition, cameras should never point into people's private residences. Generally speaking, the issue of responsible use extends to the question of the pervasiveness of these cameras. Even in a public place, having a large number of cameras may leave the consumer with no meaningful choice and render the notice ineffective since the consumer will have no choice but to pass in front of these cameras.

- *Is notice and choice the best framework for dealing with the privacy concerns surrounding these technologies, or would other solutions be a better fit? If so, what are they?*

  Notice and choice are the fundamental cornerstones and should be the basic minimum requirements. As the industry gains experience with consumer reactions, the subject needs to be revisited and other more creative protections may have to be added in due time.

- *What are best practices for developing and deploying these technologies in a way that protects consumer privacy?*

  Please see the IBIA-created document noted above and entitled *Face Detection & Face Recognition in Consumer Applications: Recommendations for Responsible Use* that defines the principles of how these applications should be deployed to protect consumer privacy. To access the document online, you may use the link provided above or you may reference the attached document.