*Before the*
**Federal Trade Commission**
Washington, D.C.

| | |
|---|---|
| | ) |
| *In the matter of* | ) |
| Face Facts: A Forum on Facial Recognition | ) |
| Project No. P115406 | ) |

## COMMENTS OF

## COMPUTER AND COMMUNICATIONS INDUSTRY ASSOCIATION

In response to the Federal Trade Commission (FTC) workshop on December 8, 2011 entitled "Face Facts: A Forum on Facial Recognition Technology" and the subsequent request for comments, the Computer and Communications Industry Association (CCIA) submits the following comments.

CCIA is an international non-profit trade association dedicated to open markets, open systems, and open networks. CCIA members participate in many sectors of the computer, information technology, and telecommunications industries and range in size from small entrepreneurial firms to some of the largest in the industry. CCIA members employ nearly half a million workers and generate approximately a quarter of a trillion dollars in annual revenue.[1]

The December workshop organized by the FTC was an excellent opportunity to begin exploring the important privacy implications of the brand new facial recognition technology. CCIA applauds the FTC for convening many stakeholders from disparate points of view and producing an informative event. We are sure that this issue will continue to get the careful consideration it deserves.

[1] A complete list of CCIA's members is available online at http://www.ccianet.org/members.

## I. Introduction

As one presenter at the workshop clearly demonstrated, the science of facial recognition is changing rapidly. What was difficult a few years ago is achievable now and the formerly impossible has become merely difficult. The technology is still new, however, and its potential applications are numerous and still growing. The attention of the FTC on the privacy implications of facial recognition is a welcome step toward making sure that the technology is implemented carefully while making sure its benefits are available to everyone.

It is likely that some uses of facial recognition technology may raise privacy concerns. Those concerns aren't all equal. Some are so mild that the majority of people might not even notice them while others may cause greater concern.

At the same time, we must be careful to avoid regulating immediately or, more importantly, too broadly. Given the youth of the industries using facial recognition technology, there is much we don't yet know about implementation details and privacy implications. In addition, it is important to recognize that there is not one monolithic facial recognition industry and therefore not one monolithic regulation that could adequately address its various uses.

CCIA hopes that the FTC will tread carefully in analyzing this emerging area, and working with all the affected stakeholders to make sure that the most is gained from this exciting new area, while at the same time working hard to recognize and mitigate the potential privacy impacts. CCIA looks forward to helping do just that.

## II. Facial Recognition is a Very Young Technology

One of the very important facts that was evident at the December workshop was how young a technology facial recognition is. While there has been ongoing research in the feasibility of computer facial recognition for some time, it is only within the past few years that consumers have had their first interactions with the realities of the technology. We encourage regulators to engage with industries using facial recognition and to monitor the possible privacy implications, but to avoid stepping in before more is known about the uses and potential harms.

As Dr. Jonathon Phillips demonstrated in his talk at the workshop and in other discussions, the National Institute of Standards and Technology has conducted multiple projects over the past 17 years aimed at helping the private research field develop facial recognition technology.[2] These projects have been aimed at improving recognition and matching of faces in varying conditions. Over that time period, the technology has made dramatic advances. For example, in 1993, the technology still failed to match two photos of the same person in similar lighting circumstances 80% of the time. By 2010, that failure rate had fallen to 0.3%.[3]

The state of the technology is worse when you take away those perfect conditions, however. In situations where the lighting is poor, the head is not facing directly toward the camera, or where a computer is attempting to analyze video, failure rates are still high enough to make positive identification unworkable. The state of the art in those conditions seems to be limited to applications like those demonstrated by the Intel AIM Suite and Scene Tap at the workshop. These implementations can attempt to predict, from video, the age range and gender of a subject.[4]

Clearly, while researchers have been working on facial recognition for more than a

[2] Jonathon Phillips, *Face & Ocular Challenges*, (2010) *available at* http://biometrics.nist.gov/cs_links/face/mbgc/MBGCFuture/BTAS_Jonathon_Phillips_Sep_2010_FINAL.pdf.

[3] Id. at 8.

[4] Using generalizations about structure and spacing of facial features, gender can be guessed, as can age group. Scene Tap, http://www.scenetap.com/. Intel Digital Signage Solutions, http://www.intel.com/p/en_US/embedded/applications/digital-signage/.

decade, commercial applications are still in their infancy, and there is still much to be done in the development of the technology. For this reason, CCIA would caution against large scale regulation and instead suggest active engagement between the various industries using facial recognition and other stakeholders, including regulators and consumer advocates. By working together, flexible solutions can be found that robustly protect privacy and encourage exploration of the new ways in which facial recognition can help users and launch businesses.

## III. Privacy Concerns and Their Impacts

There is no doubt that some uses of facial recognition technology pose privacy questions. These questions are heavily dependent on the use of the technology and the particular implementation details in each situation. Finding the right balance in each individual case is the challenge.

In situations where facial recognition technology is only being used to capture demographic data, privacy concerns are minimal. Digital signage is an example of this use. Even within this category, privacy risks could be heightened or lowered based on implementation. A system that stored the footage from the camera for some reason rather than discarding it after analysis would raise concern.

Systems that recognize a person from a face and provide the option of tagging a photo may raise a different category of privacy questions. Here, transparency and user control are important to protecting the privacy of those who might not want such a system used on their face. Here as well there are implementation details that impact privacy, such as the universe of people the algorithm searches for a match and what opportunities users have to block individual tags from attaching to photos.

In the extreme, a system that used facial recognition technology to put names and other biographical information to random faces, as is implied by the work that Alessandro Acquisti demonstrated at the workshop, carries significant privacy implications.[5] Transparency and the choice to avoid being identified would seem to be important aspects of protecting privacy in this case. Opting out of such a system raises difficult implementation questions, however, and the means of giving notice that the technology is in use would also require careful thought.

Even in this most extreme case, there are questions of implementation. If the universe of matchable people is solely the attendees at a particular conference or a party, concerns might be lessened. Limiting the universe to people the user has met before and entered into a personal database may also affect the calculus.

Overall, the privacy impacts of facial recognition technology are highly varied. They depend largely on particular uses, and even further upon individual implementations. Exploring the whole range of impacts is important work that the FTC contributed to in its workshop.

## IV. Diverse Industries and Self-Regulation

Facial recognition importantly does not represent a single monolithic industry. It is a technology that various existing industries are incorporating into their products and around which a number of new industries are growing. Regulating all uses of facial recognition broadly would ignore the important context that goes along with each use. Fortunately, we're already seeing some of those industries recognize the importance of privacy and work with consumer representatives to develop best practices and binding codes of conduct specific to each context.

The uses of facial recognition are as varied as the companies employing it. Tagging

[5] Alessandro Acquisti, *Faces of Facebook: Privacy in the Age of Augmented Reality*, 2011, *at* http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/acquisti-faces-BLACKHAT-draft.pdf.

photos based on recognized faces is one obvious implementation. Apple's iPhoto has done so for a while, and Facebook and Google+ recently announced similar features for their social networks.[6] Google's Street View product also uses facial identification to blur out the faces of pedestrians caught by the camera, preserving their privacy.[7] As seen at the workshop, facial recognition is providing advertisers with demographic data about the groups that look at their ads and even helping partygoers check how crowded a bar is before they head out the door.[8]

Each of these different uses of facial recognition carries its own privacy implications. What may be an appropriate privacy feature in one context may not make sense in another. Handing down broad rules for any use of the technology would run the risk of drastically over-regulating in some areas.

That is why CCIA is encouraged to see some of the new industries using facial recognition already getting together and developing industry privacy standards documents. One excellent example comes from the digital signage industry, which has stepped forward and developed, in coordination with consumer groups, a robust best practices document that incorporates Fair Information Practice Principles.[9] Notably, the standards were not developed in response to the threat of regulatory action, or a scandal of some kind. While they are not yet binding on members of the organization, CCIA hopes that development will continue on these standards and that they will eventually form an enforceable code of conduct. Other industries

[6] Apple – What is iPhoto, http://www.apple.com/ilife/iphoto/what-is.html. Google+ Find my Face, https://plus.google.com/101560853443212199687/posts/VV45vivcFq4. Facebook Making Photo Tagging Easier, http://www.facebook.com/blog.php?post=467145887130.

[7] Stephen Shankland, *Google begins blurring faces in Street View*, CNet News, May 13, 2008, *at* http://news.cnet.com/8301-10784_3-9943140-7.html

[8] SceneTap, *supra* note 4.

[9] Digital Signage Federation, Digital Signage Privacy Standards, 2011, *at* http://www.digitalsignagefederation.org/Resources/Documents/Articles%20and%20Whitepapers/DSF%20Digital%20Signage%20Privacy%20Standards%2002-2011%20(3).pdf.

beginning to use facial recognition should show the same leadership and begin work on similar guidelines.

## V. Conclusion

Work has already begun on exploring the privacy ramifications of facial recognition. Through industry work such as the Digital Signage Federation’s Privacy Standards, and important questions being asked by regulators, answers about best practices are beginning to emerge. CCIA is excited to see the new benefits the technology will create for consumers. Through a combination of industry self-regulation, collaboration with consumer representatives, and thoughtful Section 5 enforcement by the FTC, those benefits will flow while respecting user control and protecting privacy. CCIA looks forward to working with all stakeholders to make that a reality.