Before the
Federal Trade Commission
Washington, D.C.

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

COMMENTS OF TECHAMERICA

Chris Wilson
Director and Counsel, E-Commerce and Telecommunications
TECHAMERICA
601 Pennsylvania Ave, NW
North Building, Suite 600
Washington, D.C. 20004
(202) 682-4451

January 31, 2012

TechAmerica hereby submits these comments to the Federal Trade Commission ("Commission") in regard to the Commission's request for comment concerning facial recognition technology. A variety of TechAmerica's members utilize biometric technologies, including facial recognition, in their products and services. TechAmerica is pleased to be able to file comments on their behalf in this proceeding.

The Benefits of Facial Recognition Technology

As the Commission discovered during its recent workshop exploring facial recognition technology (FRT), FRT is currently used in a variety of contexts. Of course, recent deployments of FRT by Facebook and Google to facilitate photo tagging and social interactions have garnered a great deal of attention in the media and, indeed, at the Commission's workshop. Assuredly, understanding how FRT is used in those contexts is important. However, FRT provides benefits far beyond such uses, including for identification and authentication of individuals.

First, FRT has proven incredibly helpful to the public safety community as an identification tool. For example, police departments across the country have recently begun to utilize the Mobile Offender Recognition and Information System (MORIS), which attaches to the back of a smartphone, to effectuate arrests and identify those without traditional identification on them. MORIS utilizes FRT to analyze 130 different points on a person's face and matches that information with a central criminal database. Such "real-time" identification saves precious time and resources and has led to arrests that might not otherwise have occurred.

Of course, FRT, as a subset of biometric identification, can and does serve as a privacy enhancer by way of effectuating authentication. As the Commission likely

knows, the White House last year launched its National Strategy for Trusted Identities in Cyberspace (NSTIC) initiative. NSTIC is an effort to facilitate collaboration among industry, government, advocacy groups and others to improve the privacy, security, and convenience of sensitive online transactions. Technologies that can authenticate a user are at the heart of NSTIC. Those technologies that can leverage existing products and services, such as smartphones and smart cards, are especially important to the success and development of NSTIC. To be sure, biometric technologies are contemplated by those entities involved in the development of NSTIC. And as FRT becomes more ubiquitous along with the deployment of cameras on personal and other devices, it can be expected that FRT will be seen as an effective and voluntary alternative to the use of access passwords for online transactions. Under the right circumstances, FRT can provide the convenience, privacy and security necessary to satisfy the NSTIC vision, among other effective biometric technologies.

In evaluating the privacy implications of FRT, therefore, the Commission should be mindful of its varied uses and benefits above and beyond its application in the advertising and social media marketplace.

Providers of FRT Are Committed to User Privacy

TechAmerica appreciates the privacy concerns inherent in the use of FRT and its members are committed to ensuring that consumer privacy is balanced appropriately with innovation.

However, as a threshold matter, the Commission, when considering the privacy implications of FRT, should distinguish between facial recognition technology and facial detection technology. The latter merely recognizes a human face and provides a

general assessment of the person's age and/or gender. Facial detection technology does not uniquely identify an individual. Merchants use facial detection technology to track retail demographics in order to better allocate resources, for example. Because facial detection technology does not uniquely identify an individual, the privacy implications in its use are de minimis. For this reason, it is questionable whether users of facial detection technology need to notify consumers of its use in public spaces. Certainly, user consent for the use of facial detection technology is unnecessary.[1]

FRT, however, can be used to accurately identify a specific individual when the image is linked with one's personally identifiable information. Therefore, it is not unreasonable, where practicable, to provide consumers effective notice and choice when implementing FRT. As with any technology that impacts one's privacy, businesses have a strong interest in promoting privacy protection for FRT use. Consumer trust is paramount for effective and robust commerce. This is evidenced by the self-regulatory efforts already implemented by the Digital Signage Federation (DSF) and Point of Purchase Advertising International (POPAI). The DSF standards, in fact, are based on the Fair Information Practice Principles (FIPPs). And both the DSF and POPAI standards provide that companies must obtain consumers' opt-in consent before collecting directly identifiable information through digital signage.

Of course, TechAmerica believes that companies can and should, where possible, implement "privacy by design" throughout all applicable products, including FRT. "Privacy by design" is a concept that should be part of an accountable company's

[1] TechAmerica also questions the need for the FTC to stipulate where facial detection technology is inherently unwelcome, e.g. a public restroom, as was indicated during the FTC's workshop. Considering the fact that advertising is utilized in restrooms currently and that restrooms are already divided by gender, it is unclear why facial detection technology is de facto improper in such a venue.

overall approach to supporting privacy in an environment of technological change and information-intensive innovation. TechAmerica is confident that companies that deploy FRT take their obligations with respect to consumer privacy seriously. Indeed, self-regulation based on FIPPs coupled with "privacy by design" has provided consumers with the necessary privacy protections. Considering how relatively nascent the deployment of FRT is, especially in the consumer marketplace, it is imperative that interested observers, including the FTC, allow companies to provide innovative solutions that enable consumers to take (or not take) full advantage of the benefits of FRT.

Conclusion

TechAmerica appreciates the Commission's interest in the use and deployment of FRT. TechAmerica believes that the benefits inherent in the use of FRT, whether in social media, as an identification tool in the public safety context, or as an improved method of online authentication, far outweigh the possible negatives. Companies deploying FRT assuredly take consumer privacy seriously and must continue to do so as FRT evolves. Self-regulation and "privacy by design" have provided sufficient privacy protections so far, notably in the absence of government intervention (or threat thereof), and it is expected that such efforts will continue to mature as FRT innovation progresses in the years ahead.