Biometrics Comment to the FTC

facefacts@ftc.org

ATTN: Manas Mohaptra, Bureau of Consumer Protection
Claudia Bourne Farrell, Office of Public Affairs c/o FTC

Tuesday, January 31, 2012

RE: Comments on Biometric use concerning the public interest

Dear Mr. Mohaptra,

This is a statement of comment regarding the use of biometric technologies in identity articles, federated identity and online identity for public affairs purpose.

For the better part of 4 years, I have made an active practice supporting the public interest by: spreading notice of public input events, seeking out participation of qualified legal professionals in coalition, promoting awareness of federal programs & actions with invasive tendencies or mass surveillance potential, specifically concerning identity articles.

Biometric use with the public interest is thankfully now being carefully gauged at the Federal Trade Commission. This comes with great appreciation from myself and privacy interested constituencies on applied use of biometric technologies.

One of the greater concerns I have about the expanding biometrics market is the mandatory adoption of State required identity credentials using all forms of biometric ID, data capture and retention. The government market for biometrics is certainly suited to expand specially used identifiers with civil service and military employees for many pragmatic security purposes. However, even these publics would sustain permanent social damages if the cache of their comprehensive biometric identity was stolen or misused. There are deeper technology and legal flaws which many privacy & technology firms will iterate in their statements. I defer to more technical legal opinion at the Center of Democracy and Technology, The Electronic Frontier Foundation, The Identity Project, Privacy Activism, the Electronic Privacy Information Center, the ACLU and others in league with associated privacy and technology law as comments on these matters are made known to you.

To be brief, I am submitting key areas of greater concern with recommendations on how to bring an appropriate standard to Americans biometric identity.

There is a nagging concern over the prospect of mistaken identity or misappropriated with use of biometrics. In 2011, 4,000 US citizens were detained by ICE-DHS. 2,400 of those detained were deported last year (1). In a recent report, an IAFIS database was

referenced with detained individuals, but administrators still made discretionary mistakes. Offices using these systems jeopardised thousands of people for lack of sufficient rights toward recognition and user error. Thankfully, one step towards fixing the faulty system was installing a hotline to stop processing of inaccurately detained individuals. However, it is such a miserable “band-aid” for a process which requires deep improvement. I feel we can do better.

This was a case where the use of biometrics may have proven itself worthy. Instead, it legitimised fears that biometric identity will be bungled by State administrators who collect the ID, are careless with the proper use of the tools, information security or the long term interests of those affected by biometric mandates. How does the public make sure biometric security will be the valuable tool worth purchasing by representative governments working in their interest?

Another scenario which treads heavily upon the biometric identified person is the length of time the data is required for capture. Innovation has overcome the longevity of data when it posed a longterm problem in the past. One recommendation would be to inspire financially burdened states to eliminate resources to retain unnecessary data. Database maintenance is a burden of cost to constituents. Another would be to provide public interest materials about the type of biometrics in use and how it affects local communities.

For instance, today the FBI is piloting the Next Gen Identity system in 4 US states using a variety of biometric systems coupled with CCTV, similar to LARIAT or the UK’s Face Alert system, to test the national security benefits. However, it won’t avoid a reputation for long as an arbitrary mass surveillance device without addressing the use of the data and longevity of the data retention and relevance to the public interest. This type of system needs some sort of partnership utility agreement from the communities it will be reaching into. A highly recommended solution going forward would to stipulate each community indirectly endorsing investments in a federal biometrics system affecting mass identity would necessitate a municipal volunteer government oversight committee.

The purpose of creating of a localised oversight committee would be to ensure communities have the most comprehensive opportunity to respond to its security needs without creating a system defeating to democracy or which denies basic rights. This committee would be comprised of: citizens, NGOs, privacy law professionals, technology and budget analysts, and law enforcement. Alongside government oversight craftsmanship, would be a public interest campaign using city wide direct mailer and news releases to better inform the public of municipal changes in consideration. This would create a wider scope of awareness of each biometric program. Content would concurrently be made available online to consumers and the general public. Opportunities for public input on the problem should not be hindered by City government. Afterall, when citizens buy indirectly with federal resources they still need a way to respond as a consumer in the instance of a purchased technology becomes harmful.

The missing link in federal lawmaking seems to be municipal considerations over search & seizure of a persons identity articles as well as the costs absorbed. It should be made very clear, American society should not be lead to support a mass surveillance system with its own resources.

There are serious and obvious human rights considerations as mass surveillance systems present a psychological violence to modern societies. The burden is on the proponents of such a system to prove that their system will not create a repressive environment contrary to both US Constitutional rights and human rights and that it will be safe for public use, if mandatory. Biometric technologies are not to blame for the application. Its widespread use is very concerning, especially if applied serially to online transactions. Use of biometric identity to verify use of internet applications could be very dangerous. If bundled identity is swept together with drivers licenses, passports and other governed ID conventions it would be disastrous if stolen or misappropriated by malintents.

Federal agencies will continue to entertain private technology developers and biometric vendors to supply security tools to assist local law enforcement in intelligence gathering on citizens. There hasn't yet been much of a forum for the public to really exert opinion on government purchase of devices which could change the course of life in entire communities. Although, I have seen events sponsored by biometric companies opening the floor to the public to give input. This is considered a wan attempt at public relations over the fact that they often are pushing the adoption of their goods & services by lawful mandate vs. genuine need requests the public for their technologies. Private corporations are a largely inappropriate venue for the public to weigh in when their government is the buyer.

One application of biometrics I believe to be very unsafe going forward is the use of PICC circuitry and the collection of diverse biometric identifiers at Motor Vehicle Divisions. Motor vehicle administrators haven't fool proofed their systems to ensure privacy with data requirements in the AAMVA framework. One flaw consistently hindering information security at drivers license administrations is internal fraud. Biometric identity, if lost, stolen or mistaken, would greatly amplify the amount of risk of damage to both individuals and communities who endorse its use. Extend this misappropriation to the Internet and it would be very destructive.

There would need to be a vigilantly updated cybersecurity protocol or application used systemwide to foolproof collection of more sensitive identity data, like biometrics so that it doesn't magically get lost, sold or misapplied to someone who isn't the identified person. Motor vehicle administrators should prove success indefinitely with securing less invasive external biometrics before offering more invasive biometric records like iris captures or DNA records. As it stands, there are only funds to install these programs, not to ensure they will be safe or lessen damage to the identified person. There should be appropriate provisions for both as they are endeavored.

Finally, the biometrics industry had consistent business from the private and public sector which requires more oversight. A core problem is not as much a matter who our government purchases from, but if we truly need the goods & services we purchase at all. I urge you to investigate the processes where technology mandates become a harm to public interest. I urge the FTC to re-evaluate public-to-private business practices to reform the buying of wasteful and frequently harmful goods & services. There is much to gain in public trust by buying only what is truly needful, maintaining what is in our means.

The US government has gained a reputation for being a very wasteful government who gives business to a certain circle of "insiders" regardless of whether or not improves the the public condition. That should change. We need to reassert a proper competitive ethic; which should be subject public criticism (i.e. press) and consumer reporting. Re-evaluating policies on government contracting as a whole is a very necessary part of a conversation going forward concerning biometrics application in the public interest.

Let's continue to innovate, raise the standards of safety and quality for all Americans and US residents. It is possible to demonstrate to the public a better improved form of civics which costs less, is more secure and won't railroad their basic rights.

We can help you, if you need help to do this. Let us know how to work together.

Best,

Sheila Dean
5-11 Campaign

(1) *"And She Was An American Girl Raised on Promises (Of Due Process)"* http://ordinary-gentlemen.com/blog/2012/01/05/she-was-an-american-girl-raised-on-promises-of-due-process/