Your Mind: Legal Status, Rights and Securing Yourself

By Tiffany Rad and James Arlen

What you commonly think of as your thoughts and your mind may no longer be entirely your own. It is no longer uncommon for people to utilize electronic means to store "items to be remembered" and "actions to be undertaken" and it is fairly common for our devices to make decisions on our behalf. Our digital minions not only to help us remember things, but also can complete actions on our behalf. At what point does your computer become a legal agent able to enter into binding contracts on your behalf? How long until malware authors figure out how to exploit this new legal vulnerability? Is it reasonable to give up the legal protections for your thoughts and memories in favor of convenience? The time has come to start building rational protections for our minds before we accidentally abdicate responsibility for our Self.

There are two major types of digital memory associated with you – that which is remembered for you and that which you have some control over.

You shed digital footprints every day. Using similar technologies to the ones that track you, it is becoming easier to trace those footprints back to you. If you live in a city in which usage of video surveillance has become widespread, your image and travel patterns are often recorded and stored. In London, there is 1 camera for every 14 people and an average Londoner is seen on camera 300 times each day.[i] Although the U.S. has not yet approached that number of surveillance cameras, downtown Manhattan already has 4,200 public and private sector video cameras. The NYPD plans to install 3,000 new cameras. However, not all of this video surveillance is with cameras installed and monitored by law enforcement; police departments in Baltimore, Hollywood, Houston, Memphis, Newark, San Diego, Tampa, Virginia Beach, Washington, D.C., and in many other cities are connecting to feeds from private sector CCTV systems.[ii]

While it is unlikely you will be captured on camera pointing a gun towards a child while the Google Street Image van drives by and captures your image and location (and then keeps driving)[iii], there are new cameras being descried as pre-crime detectors. You may not have a chance to pull that gun out at all, but by measuring biometrics that, according to The Homeland Security Department, are attributes you cannot easily conceal and will give away your thought process and intent. Future Attribute Screening Technologies (FAST) cameras remotely measure biometric data such as heart rate, body temperature, pheromone responses, and respiration. DHS asked 140 paid volunteers at a Maryland equestrian center to walk past FAST scanners and some subjects were asked to "…act shifty, be evasive, deceptive, and hostile." Laser radar measure their pulse and breathing rates from a distance. DHS claims that they received a 78%-80% mal-intent detection rate. [iv] FAST can also be a benefit in that it can also reveal health conditions like heart murmurs, breathing problems and stress levels; however, retrieving and storing this information in association with personally identifying information would be an invasion

of privacy. Even with assurances by a DHS science spokesman that names will never be associated with the data, it seems as if images will and must be associated with the biometric data.

Now that $2.6 million has been awarded to Draper Laboratories to make FAST portable, these cameras may be in more places than just in airport security.[v] As a result, instead of just being used for terrorism detection, a FAST purpose previously emphasized by DHS, wherever this camera may be, your mal-intent thoughts can be read before you download that song from The Pirate Bay while hopping on open wireless networks accessible from the airport lounge. You may be able to beat facial geometry scanning in Caesar's Palace with those big "prescription" tinted glasses of yours, but FAST will read your mind.

When a lot of the video feeds are from private entities, who owns the data that is captured on camera? Know that you do not. A basic tenant of privacy law is that your privacy is conditioned upon you having a reasonable expectation of privacy. You do not have a reasonable expectation of privacy while walking on a city street while talking on your cell phone, you do in your home. While the 4th Amendment protects people, not places, future precedent may be set in which place matters, too. If you are sitting in an airport lounge thinking about mal-intent ideas near a FAST camera, while your corporeal existence is in a public place, what protects your thoughts in your mind which are not reasonably exposed or exemplified in that same public space as your body?

Some people have accepted biometric surveillance as a necessary caveat to their professional work. If you work for a casino, you understand and agree to work in an environment where there is a significant amount of screening. Similar to department store theft patterns, casino theft is often committed or facilitated by casino employees. Third Eye has an RF-based security system, SATS (Security Alert Tracking System) based on a wristband biosensor from SPO Medical that monitors employee's heart rate. If the rate suddenly increases, management is alerted by an RF signal from the wristband. The premise is that if a casino employee's heart starts suddenly beating rapidly, they are likely under stress. This could be due to some emergency such as a robbery, or possibly because the employee is planning a theft.

Your digital footprints are not just shed from where your image can be recorded in public places, but you are willingly fueling a data base keyed to you with your BlackBerrry instant messages, Tweets, Google Alerts, blogging, and other fun-but-revealing social network sites using GPS tracking social networking programs such as Four Square. You are already giving out a lot of information that is being stored regarding who your friends are, yours and their geographic locations, your interests, ethnicity, and professional/educational background.

While you are Tweeting who you are, where you are, what happened in your day and, at the same time, you are viewable on camera standing outside of work while smoking (you said you'd quit!), what are your expectations for privacy?[vi] Who owns that data of you? What about that data you e-mailed through your Gmail account to someone with servers

out on an offshore platform? If you do care about your privacy, Tweeting under your real name or an account or IP address that can be traced to you is an obvious fail.

Sometimes, you do not really have a choice about the kind of information that is being gathered about you or you have a significant personal need for the recording of that information but do not want it potentially to be used against you should it ever be obtained by law enforcement. Over the last few years, Microsoft Research Labs have been developing the SenseCam – a system for supporting human memory augmentation which has proven successful in improving the memory recall of Alzheimer's patients.[vii] Likewise, many electronic medical prosthetics now include event-loggers and other diagnostic tools which can be used to determine various facts about the health of the individual, even after death.[viii] There are even purpose-built 'human black boxes' developed by NASA.[ix] Do you trust medical companies to properly secure your personal data? Does a patient have the right to view the source code of the device keeping them alive?

Of course, with every technology, there are benefits and drawbacks. In mid-June of this year, muggers were arrested after being caught on camera by Google's Street View van crew. That is a great example of the technology working to benefit society, but when the average attention span for a security guard viewing a dozen CCTV feeds peaks at only 20 minutes,[x] you are probably not going to get caught on camera. That goes for you too, mugger. [xi] We be placated by the amount of surveillance and assume that we are safer when it is really a quality issue that improves security.

The best protection for yourself? It is going to take privacy legislation requiring private and public entities to conceal personally identifying information and images, safeguards on data mining and limits to the storage of Internet usage, such as search patterns, and with whom that information can be shared or sold. The legal profession needs to catch up to the tech industry and make changes to the way in which precedent is set; for example, a time will come when even general practitioners need to understand what an Internet protocol address is and why it does not unequivocally equal identification of a suspect. Likewise, the general public should get used to encryption of their data. Without many knowing, this is already happening to their financial data transmitted over the Internet. Hopefully, more online transmission will be encrypted by default and not by an opt-in privacy setting such as Gmail requires for https.

Until then, a lot of privacy protection is up to you. Learn to encrypt, carry your RFID credit cards and passport in a shielded wallet, refrain from Tweeting and using GPS social networking sites, know that your car stores easily accessible data about your driving habits and accidents in the data recorder, and require that law enforcement accessing your computers in any electronic device—including your blood glucose or heart monitors--obtain a warrant. But if you are not keen on encryption, cannot go an hour without Tweeting your GPS location from your cell phone or are not aware of video surveillance because you were inspired by Carrie Underwood's song, *Before He Cheats* [xii] and do a number on his car, you better be sure you are not on camera when you do it. [xiii]

Your thoughts are accessible and soon will be remotely readable. Only you can protect your thoughts by using that mind to protect yourself, your company's data communication, and where you store those electronic documents and communications. As to your digital footprints you leave in public, you already PWN3D. You may choose: accept it, run for political office or donate to a privacy-oriented non-profit like the Electronic Frontier Foundation and change legislation, or change your "Find Me, Now!" ways.

---

[i] Strauchs, John J. "CCTV: Panacea or Problem," *Security Management*, August 2008.
[ii] *Ibid.* Strauchs.
[iii] http://www.flickr.com/photos/mrbeck/2523062067/
[iv] Marks, Paul, "Pre-Crime Detector Shows Promise" *New Scientist,* September 23, 2009.
[v] "Draper Labs Awarded $2.6 million Contract by DHS" *Security InfoWatch.com*, February 6, 2009.
[vi] Poulsen, Kevin, "EFF Privacy Advocate Sighted in Google Street View" *Wired*, June 11, 2008.
[vii] http://www.microsoft.com/emea/presscentre/pressreleases/SenseCamPR_130309.mspx
[viii] Parisian, Suzanne D. M.D., Barkalow, Bruce H. Ph.D., PE, CCE, and Grant, William E. M.A., M.L.I.S., "The Pathologist's Role in Preserving Implanted Cardiac Pacemakers and Defibrillators or How Not to Get Shocked!" American Association of Forensic Sciences Annual Meeting – Washington, DC. February 2008 (http://www.bhbi.com/pdf/AAFS%20Presentation%202008.pdf)
[ix] http://science.nasa.gov/headlines/y2004/07apr_blackbox.htm
[x] *Ibid.* Strauchs.
[xi] Reuters "Dutch Muggers Caught on Google Street View Camera" *Yahoo News*, June 19, 2009.
[xii] http://www.youtube.com/watch?v=vSG4Cml7HXs
[xiii] http://izismile.com/2009/04/15/20_crimes_caught_on_google_street_view_46_pics.html