Replacing Something Bad With Something Worse: Why Biometric Authentication Will Be So Creepy

by Dr. Thomas P. Keenan, FCIPS, I.S.P., ITCP

January, 2016

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

formerly **Canadian Defence & Foreign Affairs Institute (CDFAI)**

UNIVERSITY OF CALGARY | THE SCHOOL OF PUBLIC POLICY

UNIVERSITY OF CALGARY
CENTRE FOR MILITARY AND STRATEGIC STUDIES

POLICY PAPER

Replacing Something Bad With Something Worse: Why Biometric Authentication Will Be So Creepy

By Dr. Thomas P. Keenan, FCIPS, I.S.P, ITCP

January, 2016

ISBN: 978-1-927573-54-9

Executive Summary

Technology that identifies you by physical or behavioral attributes is showing up everywhere. We find biometric identification in passports, smartphones, laptop computers, and even "smart firearms" that will only fire in the hands of the registered owner. These techniques are becoming popular because biometric identification features are ubiquitous, convenient, and harder to repudiate than other forms of personal identification. Current generation systems generally use static biometric measurements such as fingerprints, facial and iris scans, and hand geometry.

We are on the cusp of a revolution that will usher in biological (e.g. heart rhythm, brainwaves), chemical (e.g. DNA, body odor), and behavioral (e.g. gestures, gait analysis) biometrics. There will also be "body modification" technologies such as magnetic ink tattoos and the password pill from Proteus Digital Health. These have already attracted the interest of tech giants including Google and PayPal. Biometrics will also play an increasingly significant role as one of the factors in multi-factor authentication systems.

Like all nascent technologies, advances in biometrics will bring new advantages and also new risks. The move to biometrics may even spark profound social and cultural changes. The ultimate impacts may be difficult to predict, yet we have to start thinking about them. We should also encourage system creators and implementers to follow good design principles that will bring us the benefits of secure and convenient identification, while minimizing the creepy side effects.

The earliest modern computer systems were created and operated primarily for military purposes. For example, ENIAC, completed in 1946, was "used to produce ballistics tables and refine hydrogen bomb designs."[1]

By the mid-1950s, computer systems were sprouting up in government departments, large companies and educational institutions. The IBM 704, for example, was introduced in 1954 as "a large-scale, high-speed electronic calculator controlled by an internally stored program of the single address type."[2] With a price tag in the $2-3 million range (equivalent to over $15 million in today's dollars) these mainframe computers were typically a unique resource, kept in a locked room with highly restricted access. Those seeking to use them either took physical control of the computer's console, or submitted their jobs on punched cards to be run in sequence by professional computer operators.

Figure 1. IBM 704 computer in use in 1957. Public domain image from http://dayton.hq.nasa.gov/IMAGES/LARGE/GPN-2000-001881.jpg

By the early 1960s, scientists such as Jacob T. Schwartz of New York University realized that mainframe computers were becoming so fast and powerful that they could be shared, simultaneously, among a number of users.[3] Instead of submitting card decks or taking over the computer's console, users could "time share" through devices such as repurposed KSR-33 teletype machines. Projects including MIT's Multics and Control Data Corporation's KRONOS

[1] "Application: Military/Aerospace", Marketing Brochures Collection in the Computer History Museum, Mountain View, CA, accessed December 9, 2015 at http://www.computerhistory.org/brochures/applications.php?application=thm-42c167ac6dd22

[2] IBM Type 704 Manual of operation, Form 24-66661-1, IBM, 1956, accessed October 18, 2015 at ,http://www.cs.virginia.edu/brochure/images/manuals/IBM_704/IBM_704.html IBM 704 Manual of Operation

[3] Harrison, Malcolm, C., Schwartz, Jacob T., 1967. "Sharer: A Time Sharing for the CDC 6600", Communications of the Association for Computing Machinery, vol. 10, no. 10, p. 659-665.

operating system further extended this capability. The author worked on both of them at the University of Calgary, in the capacity of Systems Programmer.

Co-mingling the data of different users simultaneously on the same computer created a new risk – inadvertent or deliberate access to another user's data. For a brief period of time, a kind of "honor system" with respect to computer resources was employed, but it was soon abandoned in favor of enforced usernames and passwords. Decades later, we are still using this rather primitive security mechanism, even in the most sophisticated cloud computing environments.

The Password System is Seriously Broken

Computer security experts are virtually unanimous in criticizing the username/password paradigm. They point to human tendencies to choose simple passwords, to write them down, and to re-use the same password on multiple sites.

Industry observer Dan Tynan, writing in PC World, notes that "passwords have become self-defeating, often impotent tools in the grand scheme of digital security. We need too many of them, and the strong ones are too hard to remember."[4] He observes that we are continually being pestered to make our passwords "stronger" by adding special characters, upper and lower case letters and numbers.

New research shows that performing password gymnastics probably does nothing to make our information more secure, and may even give us a false sense of security. Two European researchers recently reported that best practices for passwords promulgated by most system operators, such as regularly changing your password, "are generally based on heuristic rules designed to defend against obsolete brute force attacks."[5]

Real-world bad guys do not grind through every possible password anymore. Instead, they use leaked lists of passwords from hacked sites, and count on the human tendency to re-use a password across different websites. If the cybercriminals obtain your password to ashleymadison.com, you can be sure they will try it on banking sites to see if you were foolish enough to use it there as well.

Security expert Bruce Schneier explains that the best way to choose good passwords is to study how people, often using automated tools, actually attempt to crack passwords. He reports on an *Ars Technica* experiment in which password cracking experts were given a file with 16,000 encrypted passwords to attack. "The winner got 90 percent of them, the loser 62 percent – in a few hours," Schenier writes.[6] He goes on to add that "a good password cracker will test names and addresses from the address book, meaningful dates, and any other personal information it

[4] Tynan, Dan, 2012. "How to Find Happiness in a World of Password Madness", PC World, Sept. 18, 2012, accessed October 26, 2015 at http://www.pcworld.com/article/2010058/password-management-future-technology.html
[5] Dell'Amico, Matteo, Fillipone, Maurizo, 2015. "Monte Carlo Strength Evaluation: Fast and Reliable Password Checking", CCS 2015, 22nd ACM Conference on Computer and Communications Security, October 12-16, 2015, Denver, Colorado, US
[6] Schneier, Bruce, 2014. "Choosing a Secure Password", posted on boingboing.net, accessed October 26, 2015 at https://boingboing.net/2014/02/25/choosing-a-secure-password.html

has. Postal codes are common appendages." Someone who is a high value target, such as a corporate executive (or that person's assistant) or a system administrator may have their entire online presence carefully scrutinized for password clues.

Faced with memory overload in an attempt to maintain a fleet of reasonably secure passwords, many users turn to password manager programs such as LastPass, Dashlane, and Sticky Password.

Password managers typically install themselves as a browser plug-in and, when a password is required, offer to supply the one you have saved earlier. They can be used on computers, tablets and smartphones, and often have both free and premium versions. Some even have a facility to pass on your credentials to a trusted party in the event that you are incapacitated or deceased.

Like all software, these products have vulnerabilities. If your master password is compromised, all your other passwords follow along. Password manager sites are also prime targets for hackers, and there have been successful attacks, such as the June 2015 intrusion at LastPass.[7]

Multi-Factor Authentication Can Help

Many business, government, and institutional computer systems require a second factor, such as an RSA SecurID hardware token, before allowing a user to perform sensitive transactions, such as transferring money or updating grades at a school. However, experience has shown that these physical tokens ("something you have") can be lost and stolen. Often, the malefactor obtains the security token device from the same desk drawer where the password ("something you know") was helpfully written on a piece of paper!

Another multi-factor approach is to have a confirmation code sent to the user's phone, especially when logging in from a location, device, or browser that has not been seen before. This type of security is available on sites ranging from Gmail to Facebook and Wordpress. Users are generally required to explicitly activate this extra layer of security. In the real world, only a small fraction do that. While the precise percentage is not released, a recent academic study of 100,000 Google accounts concluded that two-factor authentication "has not been adopted by more than 6.4 percent of the users".[8]

We are also moving into a world of multi-modal biometrics, as explained in the recent book by Marina Gavrilova and Maruf Monwar.[9] In fact, a "biometric tunnel" which takes input from a variety of biometric sensors already exists, in prototype form, in the lab of Professor Mark Nixon at the University of Southampton.[10]

---

[7] Siegrist, Joe, 2015. "LastPass Security Notice", July 10, 2015, accessed November 3, 2015 at https://blog.lastpass.com/2015/06/lastpass-security-notice.html/
[8] Petsas, Thanasis, et. al., 2015. "Two-factor Authentication: Is the World Ready? Quantifying 2FA Adoption," EuroSec'15, April 21–24 2015, Bordeaux, France
[9] Gavrilova, Marina, Monwar, Maruf, 2013. "Multimodal biometrics and intelligent image processing for security systems," Information Science Reference, ISBN 9781466636460
[10] University of Southampton, "Innovations in Biometric Innovation", accessed December 9, 2015 at http://60.southampton.ac.uk/innovations-in-biometric-identification/44

The Rise of Biometric Authentication, and the Legal Challenges It Poses

As Anil Jain points out in the comprehensive book he edited on this subject, "the term biometric authentication is perhaps more appropriate than biometrics…for brevity sake, we adopt the term biometrics in this book."[11] The same convention is used here.

The most prominent example of biometrics for consumers arrived when Apple introduced fingerprint-based Touch ID on selected models of its iPhone and iPad products. Despite the fact that its security was quickly broken by hackers such as Germany's Chaos Computer Club[12], it is being widely accepted and used in place of the four digit passcode that was used before by users who wanted at least a modicum of protection for their mobile phone.

Touch ID has led to an interesting legal debate in the U.S. If police seize the mobile phone of a suspected criminal, can they force the person to unlock it? Currently the answer may well depend on how it was locked – at least in the United States.

The Fifth Amendment of the U.S. Constitution forbids compelling a person to testify against himself. Similar protection is found in Section 8 of the Canadian Charter of Rights and Freedoms: "Everyone has the right to be secure against unreasonable search or seizure."[13]

As Anna E. Bodi observed in the American Criminal Law review, "Courts generally agree that divulging a password constitutes a testimonial act."[14] However, in October 2014, Virginia Circuit Court Judge Steven C. Frucci ruled that police could compel a criminal defendant to use his finger to unlock his phone.[15] While passcodes are protected by the Fifth Amendment, because they require a person to divulge knowledge, the judge ruled that fingerprints have no such protection because they are not "testimonial communication" under the law. Judges will also need to consider whether owning the finger that unlocks a phone may be self-incriminating by proving ownership of the phone in cases where that is disputed.

Bodi writes that "the privacy distinction being made between passcode and fingerprint access makes little sense" to the average person. She also notes that it is ironic that, while people generally believe fingerprints to be more secure than a passcode because they cannot be guessed, in the case of a criminal defendant, the biometric lock actually may reduce privacy.

---

[11] Jain, Anil K., et.al. eds., 2008. "Handbook of Biometrics", Science and Business Media, New York, ISBN 978-0-387-71040-2

[12] Rieger, Frank, 2013. "Chaos Computer Club breaks Apple Touch ID", accessed November 3, 2015 at http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid

[13] Canadian Charter of Rights and Freedoms, accessed December 10, 2015 at http://publications.gc.ca/collections/Collection/CH37-4-3-2002E.pdf

[14] Bodi, Anna E., 2015, "Phones, Fingerprints, and the Fifth Amendment," blog entry on American Criminal Law Review, January 21, 2015, accessed December 9, 2015 at http://www.americancriminallawreview.com/aclr-online/phones-fingerprints-and-fifth-amendment/

[15] Commonwealth of Virginia v. Baust, No. CR14-1439, at 1 (Va. 2d Cir. Ct. Oct. 28, 2014)

Behavioral biometrics have also been the subject of court cases. According to Vivek Mohan and John Villasenor, "Technology has outgrown the Supreme Court's Fifth Amendment jurisprudence."[16] They cite a 2012 case in which "FBI agents seized a phone secured by a pattern lock from a suspect in a San Diego-area prostitution investigation" and the owner refused to make his unlock gesture on the phone for them.

The FBI's affidavit explained their dilemma:

> To unlock the device, a user must move a finger or stylus over the keypad touch screen in a precise pattern so as to trigger the previously coded un-locking mechanism. Entering repeated incorrect patterns will cause a lock-out, requiring a Google email login and password to override. [17]

In this case, the FBI found a workaround, securing a warrant to compel Google to co-operate, thereby making the gesture entry unnecessary.

Several Canadian cases have revolved around whether or not searching the cellphone of an accused violates Section 8 of the *Canadian Charter of Rights and Freedoms*. In late 2014 the Supreme Court of Canada upheld the conviction of Kevin Fearon on charges including robbery with a firearm. The Court allowed the introduction of evidence taken from Fearon's cellphone, even though the police did not have a warrant.[18] In this case, the phone was unlocked and unencrypted, so Canadian courts will still have to face the thorny issues around devices that are protected with biometric locks.

Why Biometric Identification is Poised to Take Off

Biometric identification is not a new idea. As far back as 1892, scientist Francis Galton developed a classification system for fingerprints.[19] Many advances have been made since then, notably the 1999 introduction of the Integrated Automated Fingerprint Identification System (IAFIS) by the Federal Bureau of Investigation and the 2003 adoption by the International Civil Aviation Organization (ICAO) of biometrics into machine readable travel documents.

Today, biometrics is being promoted as a kind of "magic bullet" and, according to the Biometrics Research Group, Inc. "the global biometrics market will grow to $15 billion by 2015 from its 2012 estimated value of $7 billion."[20]

There are several factors promoting the growth of biometric identification:

- Convenience is king – you never forget to bring your finger or face

[16] Mohan, Vivek, Villasenor, John, 2012. "Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era," University of Pennsylvania Journal of Constitutional Law Heightened Scrutiny 15 (October 2012): 11-28
[17] Ibid.
[18] R. v. Fearon, 2014 SCC 77, [2014] S.C.R. 621
[19] Biometrics.gov, 2006. Biometrics History, accessed November 3, 2015 at http://www.biometrics.gov/documents/biohistory.pdf
[20] Biometricupdate.com, 2015. Accessed November 3, 2015 at http://www.biometricupdate.com/research,

- Technology is getting better, yielding better accuracy and more robustness;
- Biometrics are more difficult to copy than password or credit card numbers;
- Biometrics are difficult to share with others;
- There is actually some regard being shown for privacy, e.g. fingerprint ID systems capture key features, not the entire fingerprint;
- There are strong legal and commercial forces pushing for a "non-repudiable" identification method to secure electronic transactions.

Why Biometrics Will Have a Rocky Road

There are also a number of reasons why consumers and businesses may be hesitant to embrace biometric identification:

- It's so permanent – you are unable to change your hand geometry or retinal scan like you can a credit card number
- Edward Snowden's revelations about government tracking have made consumers suspicious of new technologies that may track them
- People are also worrying about creepy technological tracking in the commercial arena.
    - Articles such as "How Target figured out a teen girl was pregnant before her father did",[21] have raised disturbing suspicious about how we are being silently tracked on-line and in the real world of commerce.
    - Mondelez International, maker of Oreo and Chips Ahoy! cookies, is planning "smart shelves" in supermarkets. These can figure out the gender and approximate age of customers from facial biometrics.
    - Retailer Tesco is rolling out face detection to target ads at 450 locations in the UK[22]
- As pointed out in *Technocreep*,[23] it would be a small step from having in-shelf sensors to capturing a few skin cells from a keypad, which could give a company access to the ultimate biometric data – a person's DNA.

[21] Hill, Kashmir, 2012, "How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did", Forbes, February 16, 2012, accessed November 3, 2015 at http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

[22] Amscreen, 2013. Amscreen introduces digital technology to Tesco UK petrol station network,' accessed November 3, 2015 at

Some Examples of "Just around the Corner" biometric technologies

The following section provides examples of some of the more interesting biometric identification systems that are currently in development. The list is by no means exhaustive, but demonstrates that virtually every aspect of our bodies and behavior is under consideration as a possible biometric identifier.

Decisions about whether these technologies are "cool or creepy" will ultimately be made by societies, and indeed, different countries and cultures may view them differently. Here are some examples, offered without comment, in the interest of inspiring discussion.

- Scientists at the Universidad Politécnica de Madrid are claiming an 85% accuracy rate in identifying people through body odor[24]
- Researchers have found ways to identify us through the characteristics of our lips[25] (but few people want to kiss an ATM machine)
- Gait analysis is being used from military spy satellites to identify people by the way they walk.[26]

- Nymi, a Toronto-based company, plans to identify people by their unique heart rhythms

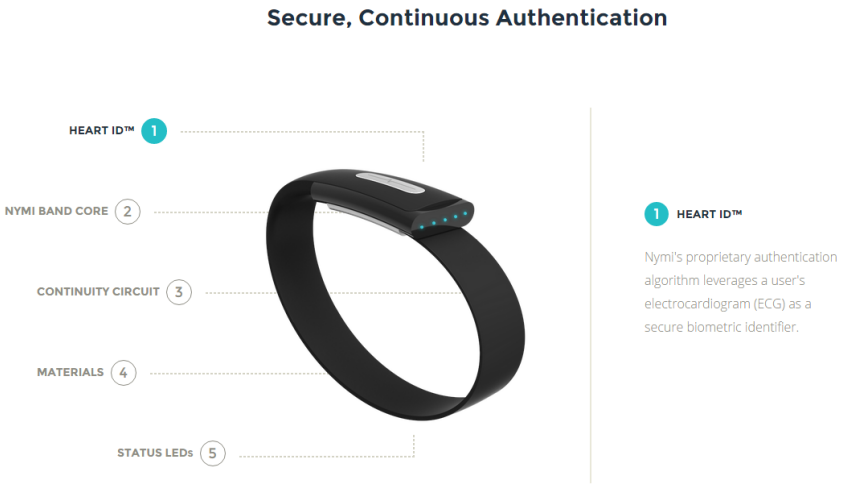


Figure 2. NYMI Heart ID™ Source: nymi.com

[23] Keenan, T.P. 2014. *Technocreep: The Surrender of Privacy and The Capitalization of Intimacy*, Greystone Books, Vancouver BC, OR Books, New York. ISBN 978-1-939293-40-4
[24] Coxworth, Ben, 2015. "Hey that smells like Frank – body odor ID is on the way", Gizmag, February 4, 2014, accessed November 3, 2015 at http://www.gizmag.com/body-odor-biometric-identification/30718/
[25] Chroas, Michal, 2009. "Lips Recognition for Biometrics", Advances in Biometrics, Volume 5558 of the series Lecture Notes in Computer Science pp 1260-1269, Springer, 2009.
[26] New Scientist, 2008. "Shadow analysis could spot terrorists by their walk", September 3, 2008, accessed November 3, 2008 at https://www.newscientist.com/article/mg19926725-800-shadow-analysis-could-spot-terrorists-by-their-walk/

- Vivalnk is already selling NFC (near field communication) temporary tattoos.

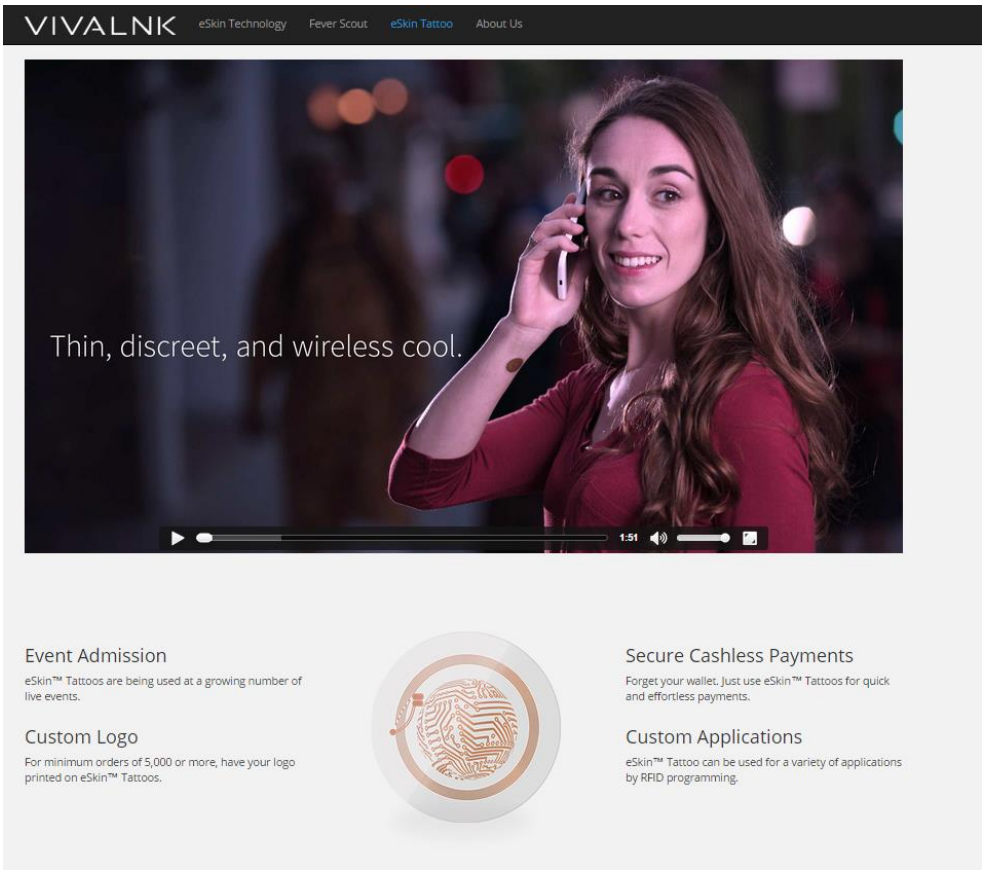


Figure 3. Digital Tattoo from Vivalnk (Source: vivalnk.com)

- Google's Regina Dugan has demonstrated a daily "password pill" which would pass through the body and send signals to unlock doors, computers, etc.[27] Interest was also demonstrated by Jonathan LeBlanc, PayPal's global head of developer advocacy.[28]

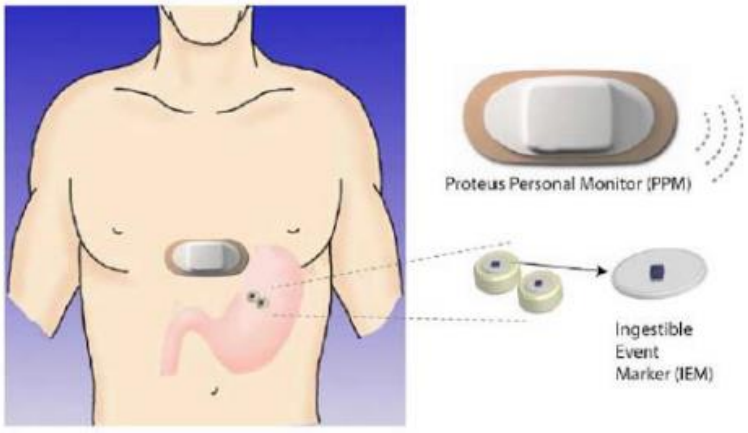


Figure 4. The "Password Pill". Concept for related product from FDA filing of Proteus Digital Health. (Source: fda.gov)

[27] Gannes, Liz, 2013. "Passwords on Your Skin and in Your Stomach: Inside Google's Wild Motorola Research Projects (Video)", AllThingsD, June 3, 2013, accessed November 3, 2015 at http://allthingsd.com/20130603/passwords-on-your-skin-and-in-your-stomach-inside-googles-wild-motorola-research-projects-video/

[28] Lamm, Jim, 2015. "Can't Remember Your Password? There's a Pill for That!", Digital Passing, May 10, 2015, accessed November 3, 2015 at http://www.digitalpassing.com/2015/05/10/remember-password-pill/

- Currently used mainly in forensic applications, Touch DNA technology will allow capture and analysis of someone's DNA from a few skin cells left behind on a surface like a water glass.

Figure 5. TouchDNA collection device. (Source: biowake.com)

Some Hidden Risks of Biometric Technology

At the Black Hat USA 2015 conference, the author presented a number of biometrics-related risks that have not been thoroughly considered by the public or technology designers. That presentation is available online,[29] and is summarized very briefly here. Consideration of these risks will be an important factor in the success or failure of new biometric identification systems.

Hidden Risk #1: Reliability, and the Public's (Mis-) Perception of It

The average user generally believes that a piece of technology either works, or it doesn't. You teach your smartphone to recognize your fingerprint and it allows you, and only you, to have access.

The truth is that biometric authentication is a statistical technique. Incomplete contact with a finger can reduce the accuracy of a fingerprint reader. Different lighting and camera angles can affect the accuracy of facial recognition. The way you walk, which is being used by some systems, can vary greatly with factors like your mood and purpose.

Hidden Risk #2: Lack of Discussion of the Consequences of Errors

In reality, biometric identification has failures like any technology. However, we do not usually give a lot of thought to the consequences of the system allowing an impostor in or rejecting a valid user.

Whether or not your iPhone's fingerprint ID recognizes you (the valid user) or accepts an imposter may or may not be consequential. If you are a doctor who urgently needs patient information stored on the device, non-access could be a matter of life or death.

Hidden Risk #3: Biometric Data's Irreversibility and the Implications

Once you grant access to certain biometric data it is generally impossible to withdraw access.[30] Additionally, the legal and privacy protection of biometric data varies widely across jurisdictions. Relevant court cases are infrequent and sometimes contradictory. However, biometric data is moving into the legal mainstream. In 2011 a California judge accepted biometric facial recognition evidence at trial, and it contributed to the conviction of defendant Charles Heard who was sentenced to 25 years to life for murder.[31]

---

[29] Keenan, T.P., 2015, "Hidden Risks of Biometric Technologies and How to Avoid Them", Black Hat USA, Las Vegas, NV, August 3, 2015, accessed November 3, 2015 at https://www.blackhat.com/docs/us-15/materials/us-15-Keenan-Hidden-Risks-Of-Biometric-Identifiers-And-How-To-Avoid-Them.pdf

[30] There has been some limited work on "cancelable biometrics" which involves distorting the biometric feature (e.g. fingerprint) before measuring it. If it is necessary to cancel that fingerprint, a new one can be created by changing the distortion parameters. See Ratha, et.al. 2001. "Enhancing security and privacy in biometrics-based authentication systems", IBM Systems Journal, vol. 40, no. 3, 2001, pp. 614-634

[31] Homeland Security Newswire, 2011. "A first: biometrics used to sentence criminal", February 1, 2011, accessed November 3, 2015 at http://www.homelandsecuritynewswire.com/first-biometrics-used-sentence-criminal

Hidden Risk #4: Our Biometrics Can Be Grabbed Without Our Consent

Simply walking in a public place exposes us to facial recognition technology, which is becoming increasingly widespread and sophisticated, often involving 3D face modelling. Companies such as Photon-X, Inc., of Kissimmee, FL advertise "standoff biometrics", which they define as the ability to collect biometric data, overly or covertly, from a distance."[32] For example, they have a non-contact fingerprint reader that works at a distance of several feet. They also offer biometric analysis of "body posture movement, gait and micro-expressions."

In a similar vein, Carnegie Mellon University engineering professor Marios Savvides has recently demonstrated a long-range iris scanning device which can zoom in on a person's eyes from a distance of six to twelve meters. It can then accurately identify them if they are enrolled in an iris-scan database.[33]

Hidden Risk #5: Our Behavior Can Rat Us Out – Sometimes Incorrectly

In addition to "things you are" biometrics can be extended to "things you do". Gestures can be used as passwords. Typing rhythm and gait (stride length, swing time) can be used to identify people. I built a prototype typing rhythm identification system in the 1980s. It could usually detect if a different person had sat down at the keyboard.

The Department of Homeland Security's "Future Attribute Screening Technology (FAST) program attempted to combine behavior and physiological factors, and was famously ridiculed at the 2011 DEF CON conference by several teenagers who pointed out why it would give many false positives.[34] The FAST system was never rolled out in U.S. airports.

In *Technocreep* I tell a story, told to me by a policer officer, about a fellow who parked his car in stall #11 of the company parking lot. He frequently said "Good Morning" to the driver who parked in stall #12, who turned out to be a Mafioso. The innocent occupant of stall #11 was put in a police computer database as a "known associate" of the bad guy!

More subtle examples include the case of a Canadian woman who was denied entry into the U.S. because of a suicide attempt. She was horrified to learn that some (but not all) Ontario police agencies were routinely putting information of this nature on CPIC (the Canadian Police Information Centre) which is available to U.S. Customs and Border Protection Agents. This caused a privacy uproar, since medical privacy was apparently being breached in an arbitrary and undocumented fashion.[35]

---

[32] Photon-X. "3D Biometric Imaging", accessed November 3, 2015 at http://photon-x.com/3D_Biometrics.html
[33] Meyer, Robinson, 2015. "Long-Range Iris Scanning is Here", The Atlantic, May 13, 2015, accessed December 10, 2015 at http://www.theatlantic.com/technology/archive/2015/05/long-range-iris-scanning-is-here/393065/
[34] Semon Rezchikov, Morgan Wang and Joshua Engelman, 2011. "Why Airport Security Can't Be Done FAST", DEFCON 19 (2011) accessed November 3, 2015 at https://www.youtube.com/watch?v=DwIlqdtr1bI
[35] Teotonio, Isabel, 2011. "Canadian woman denied entry to U.S. because of suicide attempt", Toronto Star, January 29, 2011, accessed November 3, 2015 at http://www.thestar.com/news/gta/2011/01/29/canadian_woman_denied_entry_to_us_because_of_suicide_attempt.html

Hidden Risk #6: Giving Out Biometric and Behavioral Data May Become (Possibly *De Facto)* Mandatory.

In India, the government is unapologetic about collecting your biometrics. If you want Government of India services, you must be enrolled in the world's largest biometric database, run by the Unique Identification Authority of India (UIDAI). A recent report shows that 67 percent of the country's population has been enrolled.[36]

North Americans have long resisted systems such as this, but our resolve may weaken as we see the possible benefits. Guests at some Walt Disney Resorts are being offered MyMagic™ wristbands which serve as park admission tickets as well as carrying funds for purchases. They also allow the park operator to track your every move. What rides did you go on? Where did you stop for lunch? How many times did you go to the bathroom? You *can* demand an old fashioned park admission ticket which will get you in, but you lose all the extra privileges conferred by the plastic band.

Other examples of "optional" technologies that may be so attractive they become virtually mandatory include driver tracking apps being introduced by insurance companies (Allstate's Drivesafe, Desjardins' Ajusto). Customers voluntarily give up information about their driving, including compliance with the speed limit, in exchange for a possible car insurance discount. A recent report stated that 30-40 percent of new Desjardins customers opted in for this program.[37]

Not content to simply track our driving, some insurance companies want to track our bodies. U.S. insurer John Hancock is offering discounts to some clients who wear fitness monitors.[38] New York-based provider Oscar Health Insurance actually pays its customers, up to $240 in Amazon gift cards, to reach fitness goals.[39]

Hidden Risk #7: Biometric Data Thieves and Aggregators

Like any digital data, biometric information can be stolen, tampered with, even held for ransom. It is subject to all the risk of data breaches and other crimes that might befall your banking records, payroll data, or credit card transactions.

A more subtle danger is the emergence of aggregators who cross over biometric information from multiple sources and use it to target us. Already, information that is given to 23andMe, the

[36] Times of India, 2015. "Aadhar world's largest biometric ID system", April 27, 2015, accessed November 3, 2015 at http://timesofindia.indiatimes.com/india/Aadhaar-worlds-largest-biometric-ID-system/articleshow/47063516.cms
[37] Stelmakowich, Angela, Meekbach, Greg, 2014, "Capitalizing on Change", CIP Symposium Toronto 2014, accessed November 3, 2015 at http://www.insuranceinstitute.ca/-/media/PDFs/media-releases/2014/SympoMay14ASGM%20copy.pdf
[38] CNN, 2015. "Would you wear a tracker to Get an insurance discount?", April 8, 2015, accessed November 3, 2015 at http://money.cnn.com/2015/04/08/technology/security/insurance-data-tracking/
[39] Bertoni, Steven, 2014. "Oscar Health Using Misfit Wearables To Reward Fit Customers", Forbes, accessed November 3, 2015 at http://www.forbes.com/sites/stevenbertoni/2014/12/08/oscar-health-using-misfit-wearables-to-reward-fit-customers/

direct-to-consumer DNA testing site, is being shared with Big Pharma (Genentech).[40] Although the data is supposedly anonymized and the purpose is laudable (finding Parkinson's disease drugs), the slope here is a slippery one.

A Ray of Hope

There are some reasons to be cautiously optimistic about the future of bio-privacy, at least in developed countries. Acxiom, one of the world's largest data brokers, convened a session in New York City in September 2014 around the theme of ethics as it applies to marketing data, which will increasingly include biometrics. Afterwards they produced a report that acknowledges the major changes that will be created by biometric data.

> Historically, the marketing industry had simple definitions for sensitive data. It was data about children, data about health, and data about finances. Today there are all kinds of new sensitive data, such as location data and biometric data (e.g., facial recognition data), which can be very revealing about our activities and relationships. What's more, through sophisticated analytics, companies can take data that is not sensitive at all and predict, to a high degree of accuracy, very sensitive insights about individuals, such as whether they are pregnant, what kinds of diseases they are likely to have or develop in the future, and what their financial situation is.[41]

This demonstrates a good understanding of the sensitive nature of biometric data. It will be interesting to see if the actions of this company, and others like it, live up to these principles.

Conclusion

Many of the issues raised in this paper revolve around the public's understanding and perception of biometric technologies. It is so convenient to simply look into a camera and zip through a long customs and immigration line. Yet it is unnerving to know that a theme park operator is tracking your family's every move and able to use, correlate and sell that information. Most importantly, the average citizen has little information about how biometric technologies work, and may lack the technical expertise to fully understand their functions and implications.

The short catalog of impending biometric technologies presented here illustrates the creativity of biometric systems designers, but also raises serious questions about cultural and social acceptability.

Failure to ask users "do you want this?" and "will you see this as cool or creepy?" has been a major shortcoming in technology introduction. In *Technocreep*, I proposed some "Dimensions

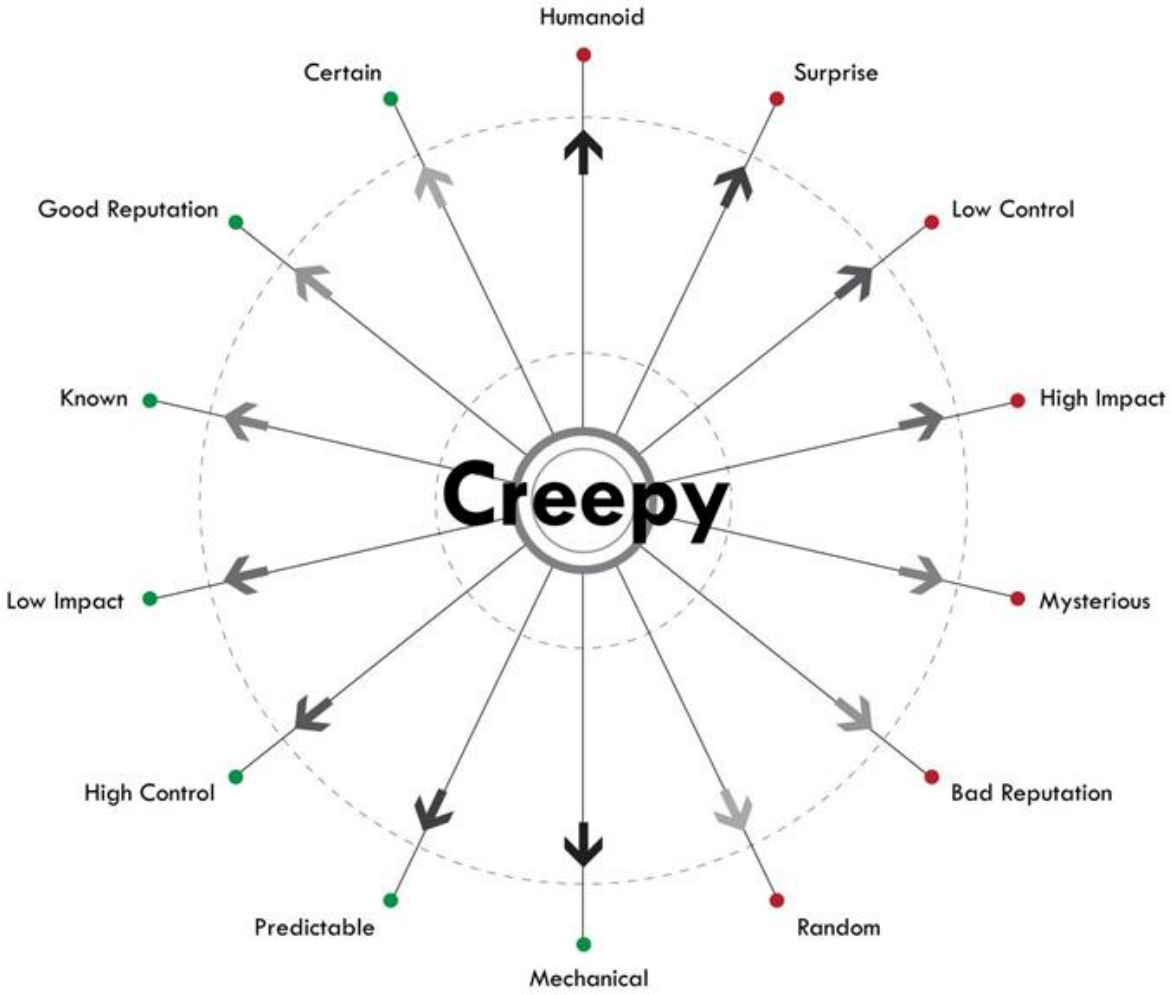
[40] Herper, Matthew, 2015. "Surprise! With $60 Million Genentech Deal, 23andMe Has A Business Plan", Forbes, January 6, 2015, accessed November 3, 2015 at http://www.forbes.com/sites/matthewherper/2015/01/06/surprise-with-60-million-genentech-deal-23andme-has-a-business-plan/

[41] Acxiom, 2015. "A Time for Action: Establishing Ethical Guidelines for Modern Data-Driven Marketing". Accessed November 3, 2015 at http://d3u9yejw7h244g.cloudfront.net/wp-content/uploads/2015/03/AC-0877-14-WP-Ethics-in-Marketing-2.pdf

of Technological Creepiness" (Appendix A) which can help to explain at least some of the public's pushback on technologies. Those who design and implement biometric technologies should be particularly sensitive to how the public will perceive their innovations, no matter how well intentioned.

Give us technologies that truly make our lives better, without making our neck hairs stand up!

Appendix A. Dimensions of Technological Creepiness (Keenan, 2014)



About the Author

Dr. Thomas P. Keenan combines a deep technical knowledge with lively insights into the social and cultural aspects of technology. He was educated at Columbia University, receiving BA, MSc, MA and EdD degrees in Philosophy, Mathematics, Engineering and Education. He is a popular professor of Environmental Design and Computer Science at the University of Calgary, a Fellow of the Canadian Global Affairs Institute and the Canadian Information Processing Society, and a Research Fellow of the Centre for Military Security and Strategic Studies. He taught Canada's first computer crime course in 1974, and was involved in drafting the country's inaugural computer crime legislation. He has been an expert witness in civil and criminal cases including one that claimed "Internet defamation".[42]

Dr. Keenan is the author of over 500 academic papers, book chapters, presentations and articles, and has spoken on five continents to academic audiences, major conferences and the general public. His 2014 book, *Technocreep: The Surrender of Privacy and the Capitalization of Intimacy* (Greystone Books, Vancouver; OR Books, New York) dissects how technology is becoming creepy in hidden ways that are difficult for most people to understand. It has appeared in the top ten on Amazon.ca in categories including Civil Rights and Liberties, Technology & Society, and Privacy.

[42] Vaquero Energy v. Weir, 2004 ABQB 68 (CanLII), <http://canlii.ca/t/1gbvd> retrieved on 2015-12-10