Hidden Risks of Biometric Identifiers and How to Avoid Them

Dr. Thomas P. Keenan, FCIPS, I.S.P., ITCP
Professor, University of Calgary
Research Fellow, Canadian Global Affairs Institute
keenan@ucalgary.ca

Abstract

Technology that identifies you by "something you are" is showing up in e-passports, laptop login screens, smart firearms and even consumer products like the iPhone. Current generation systems generally use static biometric features such as fingerprints, iris scans and facial recognition, either measured directly or mediated through a device such as a smartphone.

We're on the cusp of a revolution that will usher in dynamic (e.g., gestural, heart rhythm, gait analysis) and chemical (e.g., DNA, body odor, perspiration) biometrics. There will also be hybrid technologies such as the Nokia's vibrating magnetic ink tattoos (US Patent 8,766,784) and the password pill from Proteus Digital Health. Biometrics will also play an increasingly significant role as one of the factors in multi-factor authentication. The author created one of the first typing rhythm recognition algorithms and one of the earliest DNA sequencing machines in the 1980s and has a long term perspective on this subject.

Like all new technologies, advances in biometrics will bring new advantages and also new risks. This presentation surveys cutting edge biometric technologies and provides a framework for evaluating them from the perspectives of security, reliability, privacy, potential for abuse and "perceived creepiness". Learn what's coming down the biometrics road now, so you'll be ready to intelligently choose and implement these technologies as they come on the market in the near future.

If Biometrics is the Answer…What is the Problem?

The Username/Password System is Severely Broken

It is even the butt of jokes like the "best joke at the 2011 Edinburgh Festival":
"I needed a password eight characters long so I picked Snow White and the Seven Dwarves" – Comedian Nick Helm

However, there is a real and urgent need to accurately identify people on the Internet, especially as providers offer more high value services and allow sensitive data, such as financial and health records, to be accessed online.

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."[1]

Multi-Factor Authentication Can Help – A Bit

Many business, government, and institutional sites require a second factor, such as a SecurID fob, before performing sensitive transactions, such as moving money or updating grades at a school. However, experience has shown that 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!

With multi-factor authentication becoming available on sites ranging from Gmail to Facebook and Wordpress. Users are usually required to explicitly activate it, and, of course, only a small fraction do that.

However, it increasingly clear that "something you are" identification, such as biometrics, is useful both on its own and as part of a multi-factor scheme.

Some Reasons Why Biometrics is Poised to Take Off

Beyond the growing unease with passwords, and the inherent security problems, there are a number of additional factors promoting the growth of biometrics in the next few years.

These include:

- Convenience is king – you never forget to bring your finger or face
- Technology is getting better
- Biometrics are more difficult to copy than, e.g. passwords or CC numbers
- Biometrics are difficult to share with others

- Some attention is being paid to privacy, e.g. numbers, not full biometrics are usually collected
- Legal/Financial forces are pushing for non-repudiatable ID, e.g.
    - Oct 1, 2015: USA credit card fraud liability shifts to non-chip merchants
    - Already in Canada, a customer is unconditionally responsible for a pin verified transaction

Some Reasons Why Biometrics Will Have a Rocky Road

In the opposite direction, there are a number of reasons why consumers and businesses may hesitate to embrace biometric identification:

- It's so "you" – i.e. you can't change your fingerprint or retinal scan like you can a credit card number
- Snowden revelations about government tracking have made consumers suspicious of new technologies.
- The same holds for technological tracking by businesses, e.g.
    - "Target Knows Teen is pregnant" is a great yarn but there are more realistic predictive analytic business cases (divorce prediction; likelihood you'll switch insurers; creditworthiness via your friends)
    - FBX and the like: I'm being pursued by a wall oven and a rental car
    - "Smart shelves" in supermarkets that guess your age, gender, BMI

Biometrics is Not a New Idea!

In fact, there is evidence of hand-"signed" cave paintings dating back 31,000 years.

Practical landmarks in biometric identification as we know it now include:

- 1892 Galton develops fingerprint classification system[2]
- 1959 LAPD catalogs "tattoos and identifying marks"[3]
- 1994 First iris recognition algorithm patented
- 1994 INSPASS (automated immigration service using hand geometry) introduced
- 1994-1999 FBI develops and launches IAFIS (fingerprints)
- 1998 FBI launches CODIS (DNA database)
- 2001 Face recognition tested at Superbowl in Tampa
- 2002 Film *Minority Report* sensitizes the public to biometrics
- 2003 ICAO supports machine readable travel documents
- 2004 US VISIT program becomes operational
- 2009 India establishes Unique Identification Authority of India

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

The average user of technology generally believes that things either work, or they don't. News reports that several groups, from the Chaos Computer Club in Germany to Marc Rogers of Lookout Security, were able to trick the fingerprint biometric lock on Apple iPhones probably gave many people the impression that "biometrics is not reliable."

Yet, even Rogers concluded that:

> Just like its predecessor — the iPhone 5s — the iPhone 6's TouchID sensor can be hacked. However, the sky isn't falling. The attack requires skill, patience, and a really good copy of someone's fingerprint — any old smudge won't work. Furthermore, the process to turn that print into a useable copy is sufficiently complex that it's highly unlikely to be a threat for anything other than a targeted attack by a sophisticated individual. I'll reiterate my analogy from my last blog on TouchID: We use locks on our doors to keep criminals out not because they are perfect, but because they are both convenient and effective enough to meet most traditional threats.[4]

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

In reality, biometric identification has failures like any technology.

To quantify this, system designers talk about three kinds of error rates for biometric (and other) systems:

- Type I Error: False Reject Rate – FRR (doesn't allow valid access when it should)
- Type II Error: False Accept Rate - FAR(allows access when it should not)
- Crossover Error Rate – CER (the point at which FRR=FAR, i.e. "neutrality")

Making the system more "fussy" in a technology way can lower the FAR but at the expense of a higher FRR. Often designers aim for a balance (the CER) of False Rejects and False Accepts. However, this setting can be influenced by the possible consequences of each type of error.

Whether or not your iPhone's fingerprint ID recognizes you (the valid user) or accepts an imposter may or 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. If you store highly secret information on it, letting an imposter gain access could have very negative consequences.

In a reported weakness in a certain operational trusted traveler system, the iris-based biometrics system would sometimes fail to uniquely identify the traveler, resulting in an arbitrary and possible incorrect choice of potential passengers. Since this technology is protecting borders, that would seem to be a serious flaw. However, since all the names were drawn from a roster of carefully vetted travelers, the actual risk was probably minimal.

The real problem is that the technical parameters that govern biometric error rates are often decided by technologists, possibly informed by a few policy makers. They are rarely discussed in a public forum, partly because of the “cloak and dagger” nature of many of these systems.

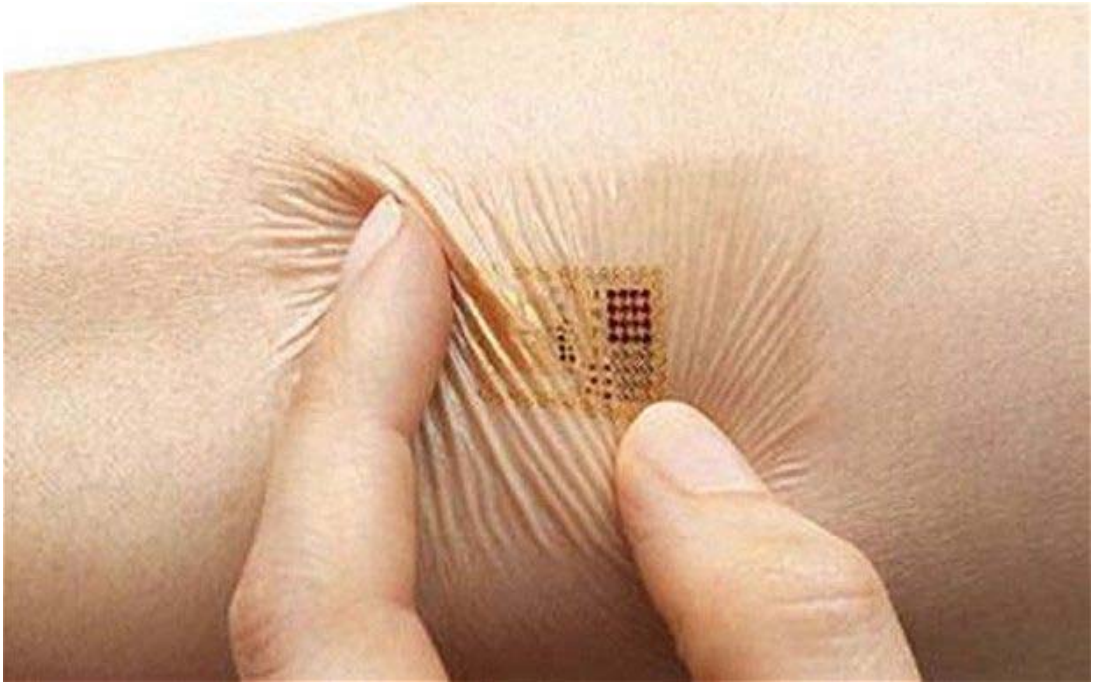
There are some exceptions. When obtaining the NEXUS frequent traveler card, which allows expedited US/Canada border crossing, applicants are told that they will still be subject to random secondary inspection at the same rate as the general public. In some cases, the percentage is even disclosed. This goes a long way towards giving the user a realistic understanding of the system they are joining.

Selected ‘Just Around the Corner’ Biometric Technologies

These are some of the biometric technologies we will be discussing in the next five years

a) Digital Tattoo from Vivalnk

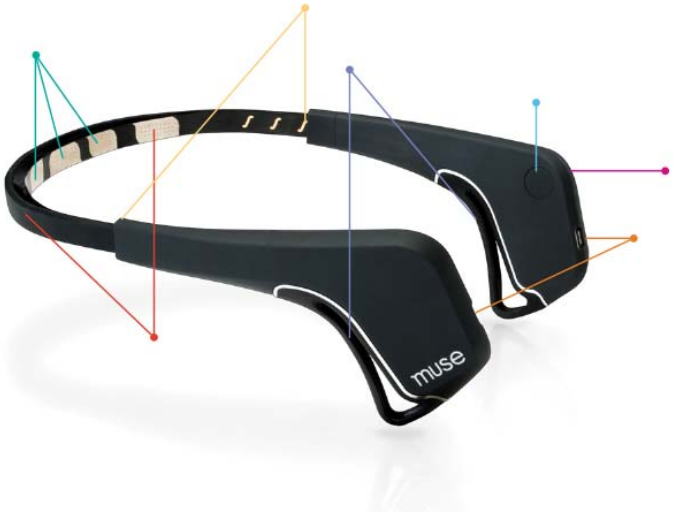
b) Motorola's patented "phone on your skin"[5]



c) Google's "Password Pill"

d) Nymi's Heart rhythm biometric identification device

e) The MUSE EEG headset which can be used to read brainwaves



F) Biowake's TouchDNA Kit

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

Once you grant access to certain biometric data, such as your DNA, it is generally impossible to withdraw access.[6] Even if the data is cared for diligently, and only portions are retailed e.g. yes/no for selected DNA markers (single nucleotide polymorphisms), there is a danger of "data jigsawing" with other databases.

In addition, the legal protection of biometric data varies widely across jurisdictions, and court cases are infrequent and sometimes contradictory. However, it is worth noting that in 2011 a California judge accepted biometric facial recognition evidence and it contributed to the sentencing of defendant Charles Heard to 25 years to life for murder.[7]

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."[8] 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."

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 reasonable typing rhythm 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.[9]

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 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.[10]

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

In India, it's clear. 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% of the entire population has been enrolled.[11]

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. Imagine telling your 7-year old nice "Yes, Sally, that family is going to the front of the line, but we will wait here in the blazing sun for an hour – because we value our privacy!"

Other examples of "optional" technologies that may be so attractive they virtually mandatory include the driver tracking apps (Allstate's Drivesafe, Desjardins' Ajusto). People 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% of new Desjardins customers opted in for this program.[12]

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. It has also been noted that fitness monitors can determine things like when you are having sex and how many hours you slept last night. If an airline pilot shows up for work on the wrong side of that equation, it might make sense to ground him or her. What if the person is doing a menial job? Who should decide about fitness to work?

Hidden Risk #7: Biometric Data Thieves and Aggregators

Biometric information is bits like any other digital information. It can be altered, stolen, even held for ransom. It is subject to all the data breaches and other crimes that might affect your banking information or school records.

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 direct-to-consumer DNA testing site is being shared with Big Pharma (Genentech).[13] Although the data is supposedly anonymized, and the purpose is noble (finding Parkinson's disease drugs,) the slope is a slippery one.

There is a bit of hope here. Acxiom, one of the world's largest data brokers and marketing companies has the following statement on their website:[14]

> **Employing Sensitive Data for Marketing and Advertising**
>
> 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.

Those are noble words, and they show 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

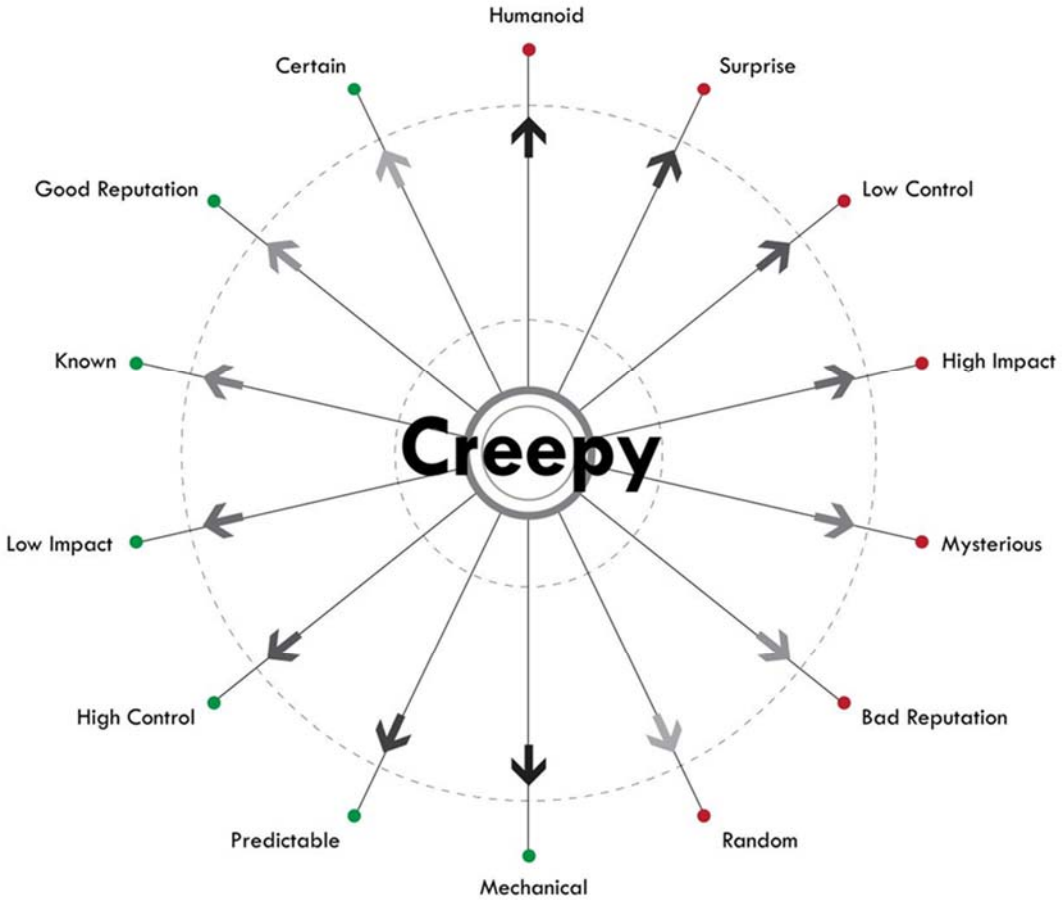
Many of the issues raised in this paper revolve around the public's understanding and perception of biometric technologies. It can be delightful to flash your eyes and zip through a long immigration line. Yet it is unnerving to know that a theme park operator is tracking your family's every move and using or even selling that information.

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 of 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 – Technocreep Factors (Keenan, 2014)[15]

"Dimensions of Technological Creepiness"



References

[1] www.biometricupdate.com/research, accessed April 15, 2015
[2] www.biometrics.gov/documents/biohistory.pdf,
[3] Keenan, T.P. 2014. ***Technnocreep: The Surrender of Privacy and The Capitalization of Intimacy***, Greystone Books, Vancouver BC, OR Books, New York. ISBN 978-1-939293-40-4
[4] blog.lookout.com/blog/2014/09/23/iphone-6-touchid-hack/
[5] USPTO, US Patent No. 2013297301, "COUPLING AN ELECTRONIC SKIN TATTOO TO A MOBILE COMMUNICATION DEVICE," Alberth, JR, Williams, P, assigned to Motorola Mobility Inc.
[6] There is a concept of "cancelable biometrics" that work via distortion of biometric features such as fingerprints
[7] http://www.homelandsecuritynewswire.com/first-biometrics-used-sentence-criminal
[8]http://photon-x.com/3D_Biometrics.html
[9]

https://www.youtube.com/watch?v=DwIlqdtr1bI
[10] Teotonio, Isabel. "Canadian woman denied entry to U.S. because of suicide attempt," Toronto Star, January 29, 2011, accessed at http://www.thestar.com/news/gta/2011/01/29/canadian_woman_denied_entry_to_us_because_of_suicide_attempt.html
[11] http://timesofindia.indiatimes.com/india/Aadhaar-worlds-largest-biometric-ID-system/articleshow/47063516.cms
[12] http://www.insuranceinstitute.ca/-/media/PDFs/media-releases/2014/SympoMay14ASGM%20copy.pdf
[13] http://www.forbes.com/sites/matthewherper/2015/01/06/surprise-with-60-million-genentech-deal-23andme-has-a-business-plan/
[14] http://www.acxiom.com/resources/time-action-establishing-ethical-guidelines-modern-data-driven-marketing/
[15] Keenan, T.P., *op. cit.*