

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

Las Vegas, NV August 3, 2015



IN THE NEXT HOUR, YOU WILL LEARN

- Why biometrics are about to become very important in your job and your life
- How it will have subtle consequences that people aren't talking about yet
- Some creepy biometric ideas that are “just around the corner”
- How you can get ready for the biometric revolution
- But first, if biometric technologies are the solution -- what is the problem?

HOW BAD IS THE “PASSWORD PROBLEM”?

I remember when your password was physical possession of the computer!



NOW COMEDIANS MAKE JOKES ABOUT THEM, AND USERS ARE FRUSTRATED

- “I needed a password eight characters long so I picked Snow White and the Seven Dwarves” – Comedian Nick Helm
- Computer: Please enter a new password
User: cabbage
Computer: Sorry, the password must be more than 8 characters

User: boiled cabbage

Computer: Sorry, the password must contain 1 numerical character

User: 1 boiled cabbage

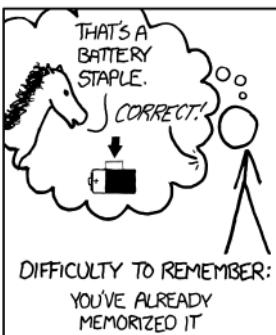
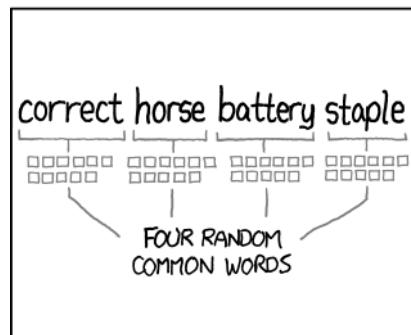
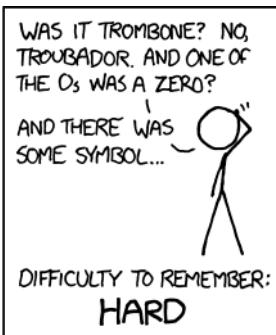
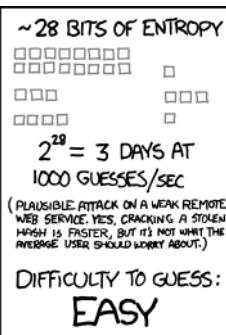
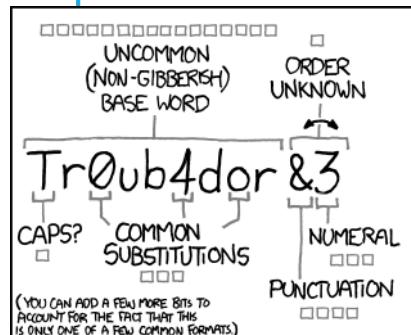
Computer: Sorry, the password cannot have blank spaces

/* time passes and much effort is expended */

User:NowIAmGettingReallyP****dOff50F***ingBoiledCabbagesShove
dUpYourA**IfYouDontGiveMeAccessImmediately

Computer: Sorry, that password is already in use!

AND OF COURSE XKCD WEIGHS IN

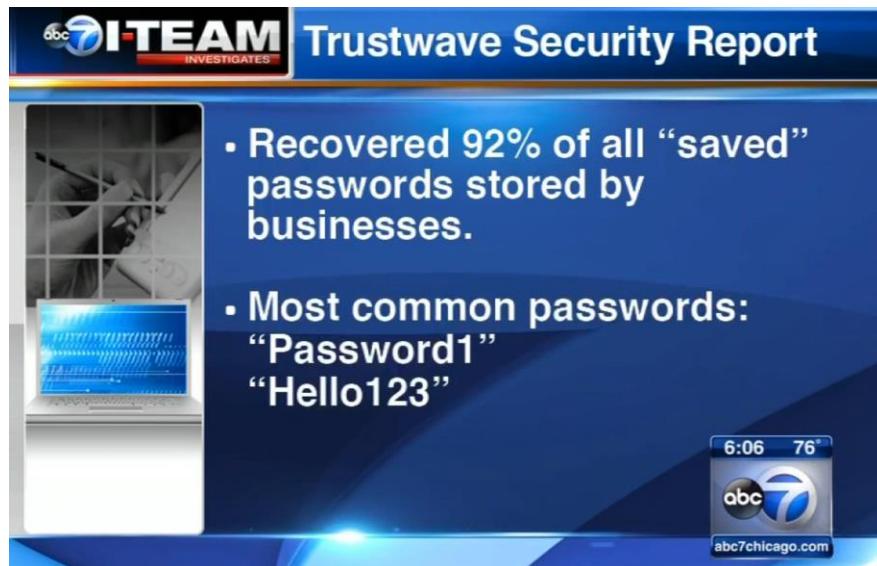


THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.



Source: xkcd.com under CC BY-NC 2.5

YES, THERE'S STUPIDITY, BUT THERE'S MORE



abc 7 I-TEAM INVESTIGATES Trustwave Security Report

- Recovered 92% of all “saved” passwords stored by businesses.
- Most common passwords:
“Password1”
“Hello123”

6:06 76° abc 7abc7chicago.com

A graphic from an ABC 7 Chicago news segment titled "I-TEAM INVESTIGATES Trustwave Security Report". It features a blue background with a small image of a person working at a desk on the left. The main text area contains two bullet points about password recovery and common passwords. A news ticker at the bottom shows the time as 6:06 and the temperature as 76°, with the ABC 7 logo and website address abc7chicago.com.

Russian Hackers

- 1.2 Billion
- User Names & Passwords
- From 420,000 Websites

6:04 76° abc 7abc7chicago.com

A graphic from an ABC 7 Chicago news segment titled "Russian Hackers". It features a blue background with images of a computer monitor, keyboard, and tablet. The main text area contains three bullet points about the scale of the hack. A news ticker at the bottom shows the time as 6:04 and the temperature as 76°, with the ABC 7 logo and website address abc7chicago.com.

Source: <http://abc7chicago.com/technology/i-team-protecting-usernames-passwords/245303/>

BIOMETRICS IS POISED FOR HUGE GROWTH

Biometrics Research Group Inc. projects that the global biometrics market will grow to \$15 billion by 2015 from its 2012 estimated value of \$7 billion.
(www.biometricupdate.com/research)

It is moving into every sector from banking to healthcare to retail, and will play a "killer app" role in enabling mobile commerce

WHY BIOMETRICS WILL RULE THE WORLD

Passwords are indeed severely broken

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

Some attention is being paid to privacy, e.g. hashes and not full biometrics are usually collected

Legal/Financial forces are pushing for non-repudiable ID

- Oct 1, 2015: USA Fraud liability shifts to non-chip merchants
- Already in Canada: consumer liable if PIN entered

WHY BIOMETRICS WILL CREEP PEOPLE OUT

It's so "you" – you can't change your fingerprint or retinal scan like you can a credit card number

Snowden revelations about Government Tracking

Business Tracking:

- "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

A VERY BRIEF HISTORY OF BIOMETRICS

- 31,000 years ago: Handprint “signed” cave paintings
- 500 BC Fingerprints on Babylonian clay tablets
- 1892 Galton develops fingerprint classification system
- 1959 LAPD catalogs “tattoos and identifying marks”
- 1994 First iris recognition algorithm patented
- 1994-1999 FBI develops and launches IAFIS (fingerprints)
- 1998 FBI launches CODIS (DNA database)
- 2001 Face recognition tested at Superbowl in Tampa
- 2003 ICAO supports machine readable travel documents
- 2004 US VISIT program becomes operational

Sources: <http://www.biometrics.gov/documents/biohistory.pdf>, last updated August 2006
www.tattooarchive.com/tattoo_history/identification.html



Source: Wikimedia Commons under CC BY-SA 3.0

Nexus: Canada's Trusted Traveler Program

MP LOIS BROWN ANNOUNCES NEW TRUSTED TRAVELLER KIOSK

February 29, 2012



“Original” Nexus Kiosks

- Were often broken
- Ambitious idea...but...
a “glitch”
- Want one? =====>

Item Details

Information

Sold For:	\$155.01
Item:	3 Nexus Kiosks
Closing Date:	29-April-2015 @ 10:53 a.m. EASTERN TIME
Quantity:	3 (each)

Description: Nexus kiosks

Description :

- Dimensions for each kiosk
 - 0.91 meters wide
 - 0.91 meters deep
 - 1.37 meters high
- Weight 227 kg
- These dimensions do not include the overhead electronic display screen and additional pieces
- All hard drives have been removed.
- In working condition when taken out of service.

Additional Comments:

1. For information and an appointment to view, please call the contact listed OR **Richard Gagnon** 613-960-3581 RichardA.Gagnon@cbsa-asfc.gc.ca
2. **Contact-person for inquiries specific to kiosks :** **Christine Amyotte** 343-292-5642 Christine.Amyotte@cbsa-asfc.gc.ca
3. Appointments to view and pick-up are mandatory, no exceptions.
4. The entire lot must be picked up in a single trip.
5. Purchaser must come equipped and prepared with proper equipment to pick up the lot from the building, example: dollies, carts, vehicle and/or trucks, as well as proper amount of staff/help for the move.
6. Purchasers who arrive unprepared will be refused.
7. 4-foot-high loading dock with electric metal plank behind unit H at 2405 St Laurent

Pictures



HIDDEN RISK #1: BIOMETRIC RELIABILITY AND THE PERCEPTION OF IT

- WE know that technology is only right some of the time
- The general public sees it as “all or nothing”

September 23, 2014

Why I hacked TouchID (again) and still think it's awesome

By Marc Rogers 11 Comments

 Recommend 190

 Tweet 234

Last year, when the iPhone 5S was released, I showed how you could hack its fancy new TouchID fingerprint sensor. A year and one iPhone 6 later, I've done it again.

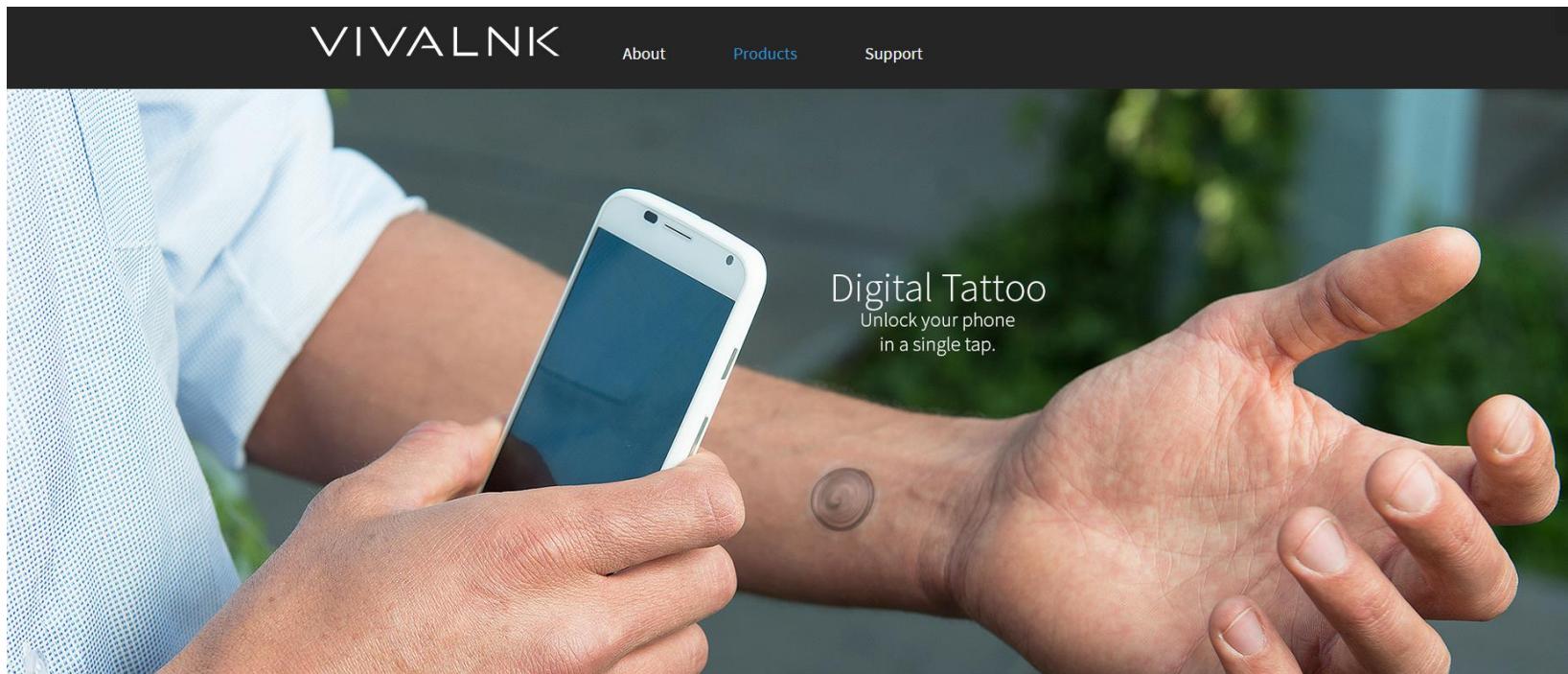
Conclusion

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.

HIDDEN RISK #2: LACK OF DISCUSSION OF THE CONSEQUENCES OF ERRORS

- In Biometrics, by convention:
 - Type I Error: False Reject Rate (doesn't allow valid access)
 - Type II Error: False Accept Rate (allows access when it should not)
 - Crossover Error Rate (point at which $FRR=FAR$, “neutral”)
- Consequences of your iPhone not recognizing you or accepting an imposter? It depends!
- Consequence of the Nexus terminal mis-identifying travelers?
Probably low since they were all on the trusted traveler list to begin with
- The point is that Type I and Type II errors are usually hidden in technical specs (if they are considered at all) but can have important policy implications

ID TECH IS ALREADY GETTING ~~UNDER~~ON, OUR SKIN

A photograph showing a person's arm and hand. They are holding a white smartphone in their left hand and using their right index finger to tap a small, circular, transparent digital tattoo placed on their forearm, just above the wrist. The background is blurred green foliage.

VIVALNK

About Products Support

Digital Tattoo
Unlock your phone
in a single tap.

Source:
vivalnk.com

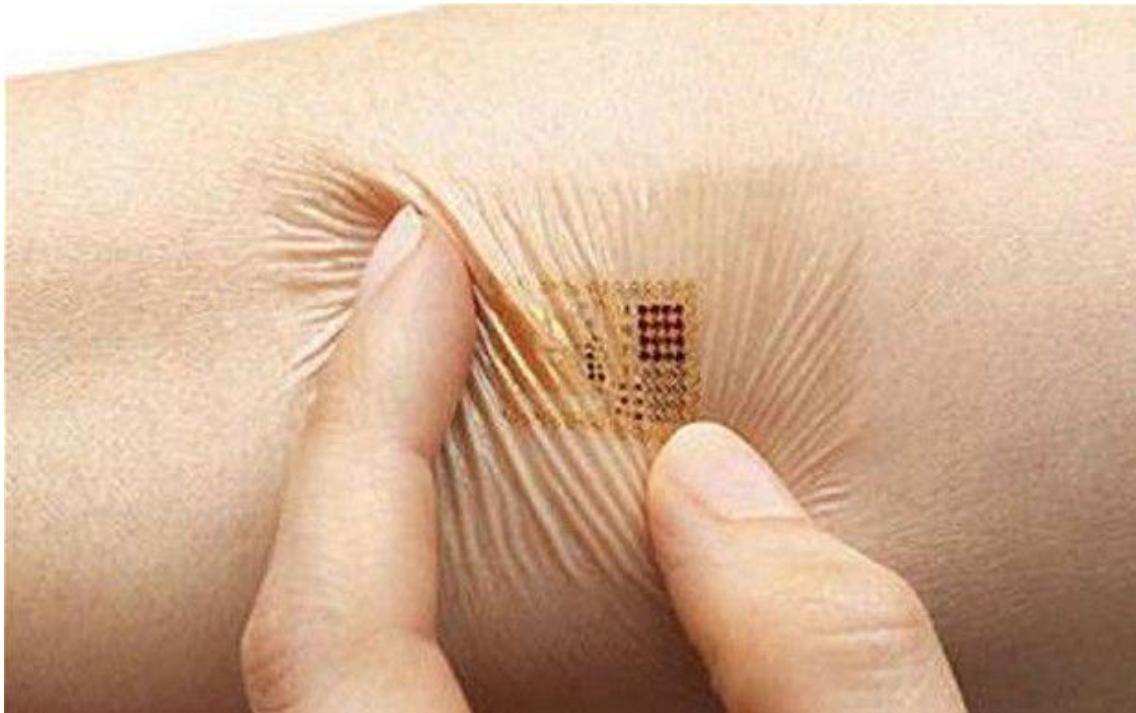
BUY NOW \$9.99



UNIVERSITY OF
CALGARY



THEY'RE EVEN CLAIMING A "COOL FACTOR"



That's a
microphone!

Source: IC10, via
telegraph.co.uk

AND, IT'S PATENTED TECHNOLOGY

US PATENT & TRADEMARK OFFICE PATENT APPLICATION FULL TEXT AND IMAGE DATABASE



(6 of 9)

United States Patent Application

20130297301

Kind Code

A1

Alberth, JR.; William P.

November 7, 2013

COUPLING AN ELECTRONIC SKIN TATTOO TO A MOBILE COMMUNICATION DEVICE

Abstract

A system and method provides auxiliary voice input to a mobile communication device (MCD). The system comprises an electronic skin tattoo capable of being applied to a throat region of a body. The electronic skin tattoo can include an embedded microphone; a transceiver for enabling wireless communication with the MCD; and a power supply configured to receive energizing signals from a personal area network associated with the MCD. A controller is communicatively coupled to the power supply. The controller can be configured to receive a signal from the MCD to initiate reception of an audio stream picked up from the throat region of the body for subsequent audio detection by the MCD under an improved signal-to-noise ratio than without the employment of the electronic skin tattoo.

Inventors: Alberth, JR.; William P. (*Prairie Grove, IL*)

Applicant: Name City State Country Type

Alberth, JR.; William P. Prairie Grove IL US

Assignee: MOTOROLA MOBILITY, INC.

Libertyville

IL

Family ID: 48468791

Appl. No.: 13/462881

Source: uspto.gov

“GOOGLE’S CREEPIEST IDEA EVER”

The Swallowable Pill That Makes You Into a Human Password



Slate



Source: slate.com

HERE COME THE DIGITAL BLOODHOUNDS

Body odor as a biometric identifier

Researchers at the UPM along with the Ilía Sistemas company are making progress on the development of a new biometric technique that would allow us to identify people through their personal odor.

The research of the Group of Biometrics, Biosignals and Security (GB2S) of the Universidad Politécnica de Madrid (UPM) in collaboration with Ilía Sistemas SL unveils that there are recognizable patterns of each person's body odor that remain steady. Therefore, every person has his/hers own odor and this would allow his/her identification within a group of people at an accurate rate higher than 85%. This result leads the way to improve personal identification that is less aggressive than other biometric techniques being used today.

Nowadays, our identity verification in most airports or border checkpoints is based on our physical resemblance to our ID card or passport photo. Even though the new electronic passports are difficult to forge, the usage of biometric techniques based on a person's physical features would increase the safety effectiveness of the border control checkpoints.

Source: UPM

Several biometric techniques like the iris and fingerprint have a low error rate. However, these two techniques are usually related to criminal records and for this reason when a person is required to identify himself is reticent to collaborate. On the other hand, other recognized biometric techniques like the face recognition have a high error rate. Therefore, the development of new sensors that allow the capture of body odor can provide a less aggressive solution because the identification could be at the same time when crossing the system stall.



Source: Universidad
Politécnica de Madrid ©
2015

DOES LOGGING ON MAKE YOUR HEART SKIP A BEAT?

YOUR EVERYDAY SIMPLIFIED

Seamlessly unlock devices, remember passwords and more, using your heart's unique signature.

[RESERVE NOW](#)

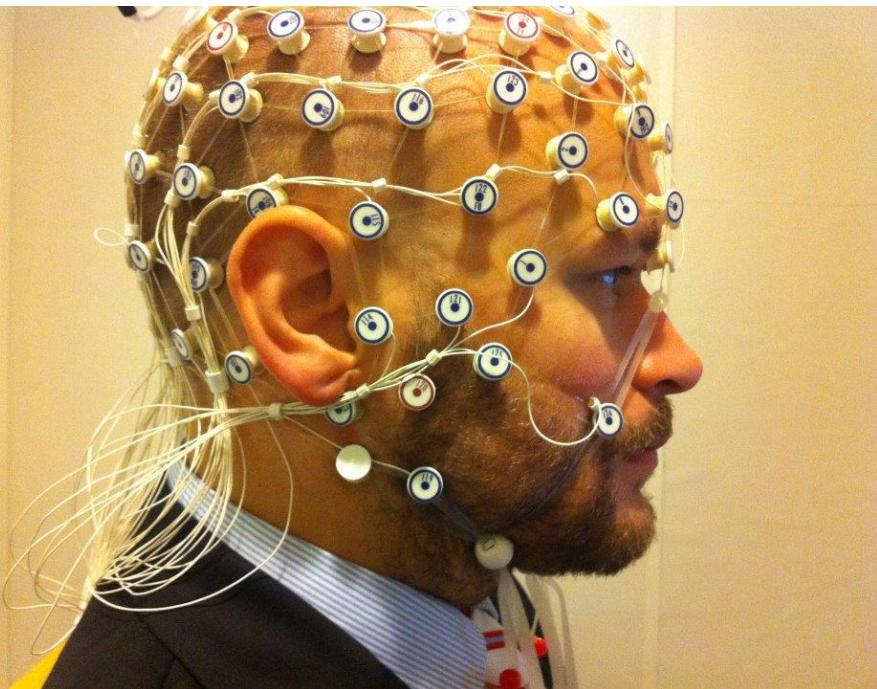
[WATCH VIDEO ▶](#)

 nymi band™

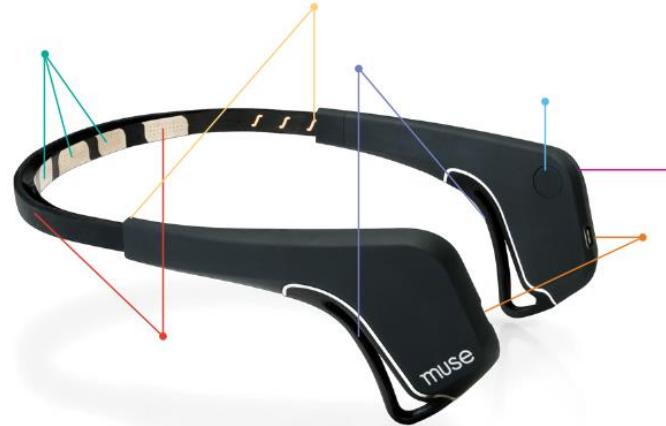


Source: nymi.com

IF NOT YOUR HEART RHYTHM... YOUR EEG



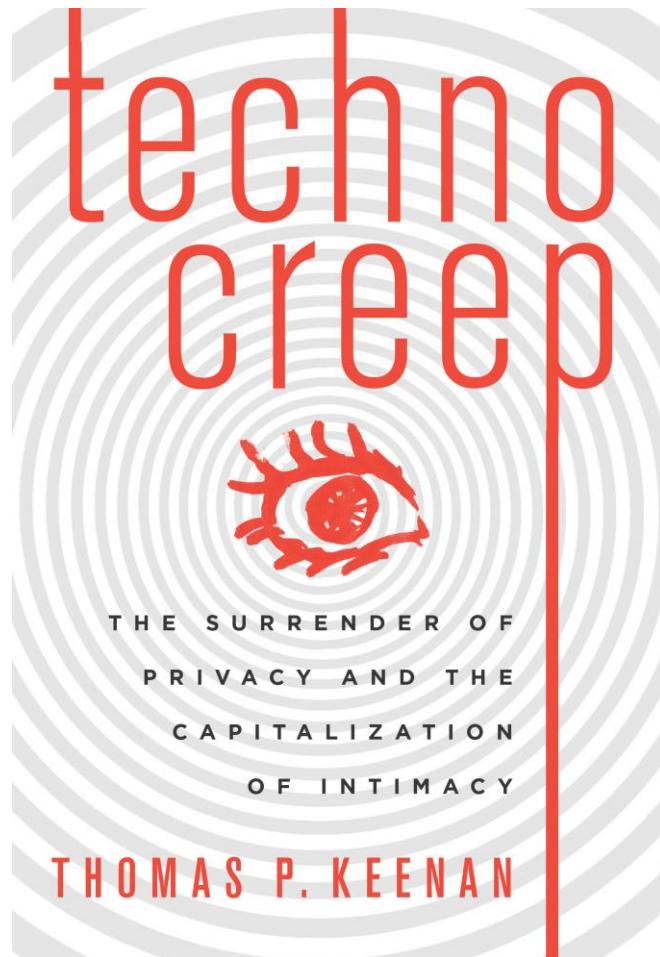
- Neurosky
- OpenEEG
- Emotiv
- Muse



Source: Wikipedia

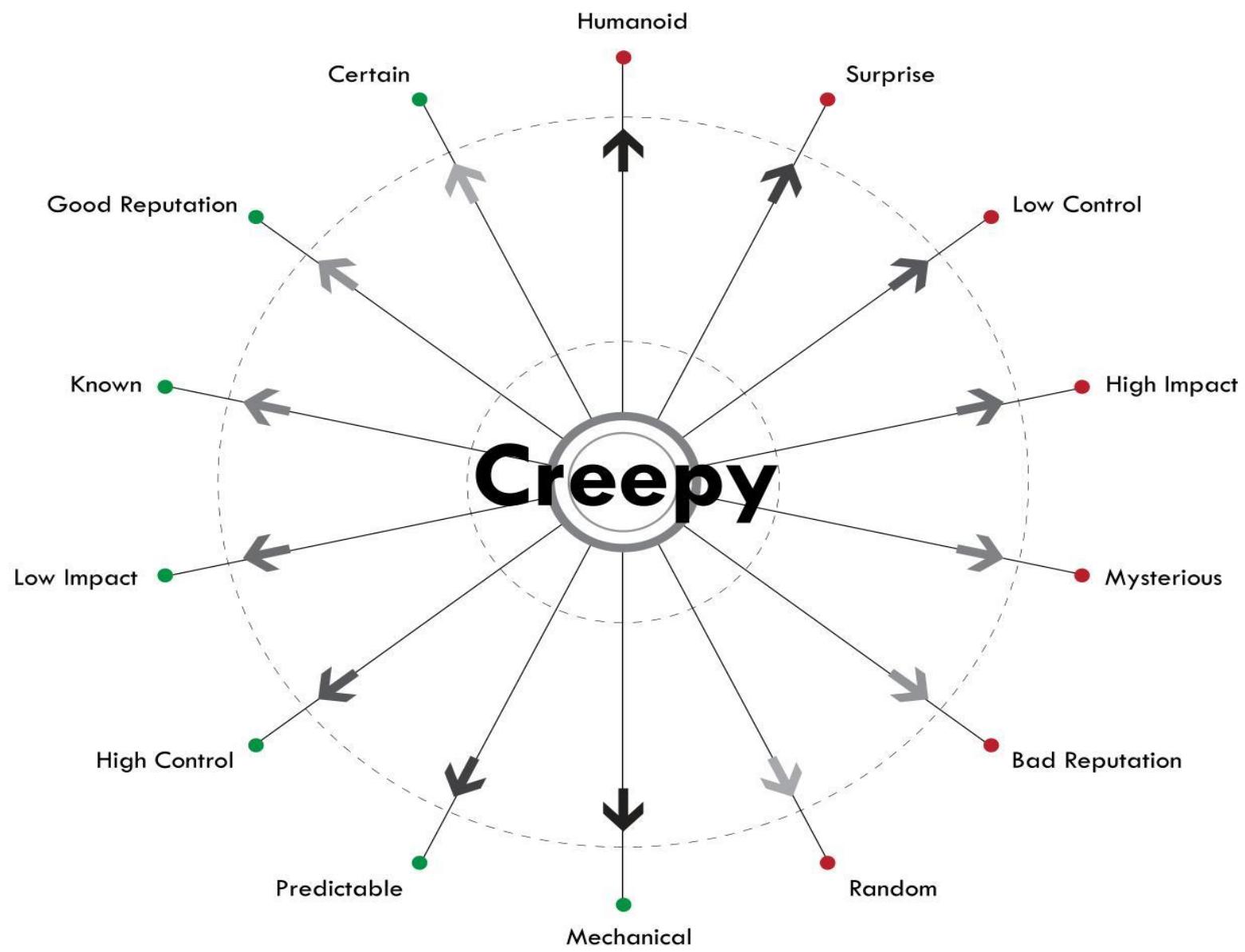
MY RESEARCH INTO TECHNOCREEPINESS

- There are “wheels within wheels”
- Most people don’t, and perhaps can’t understand exactly what’s going on



- Still, they have an uneasy feeling
- Laws and regulations are lagging

“Dimensions of Technological Creepiness”



A Philosophical Example

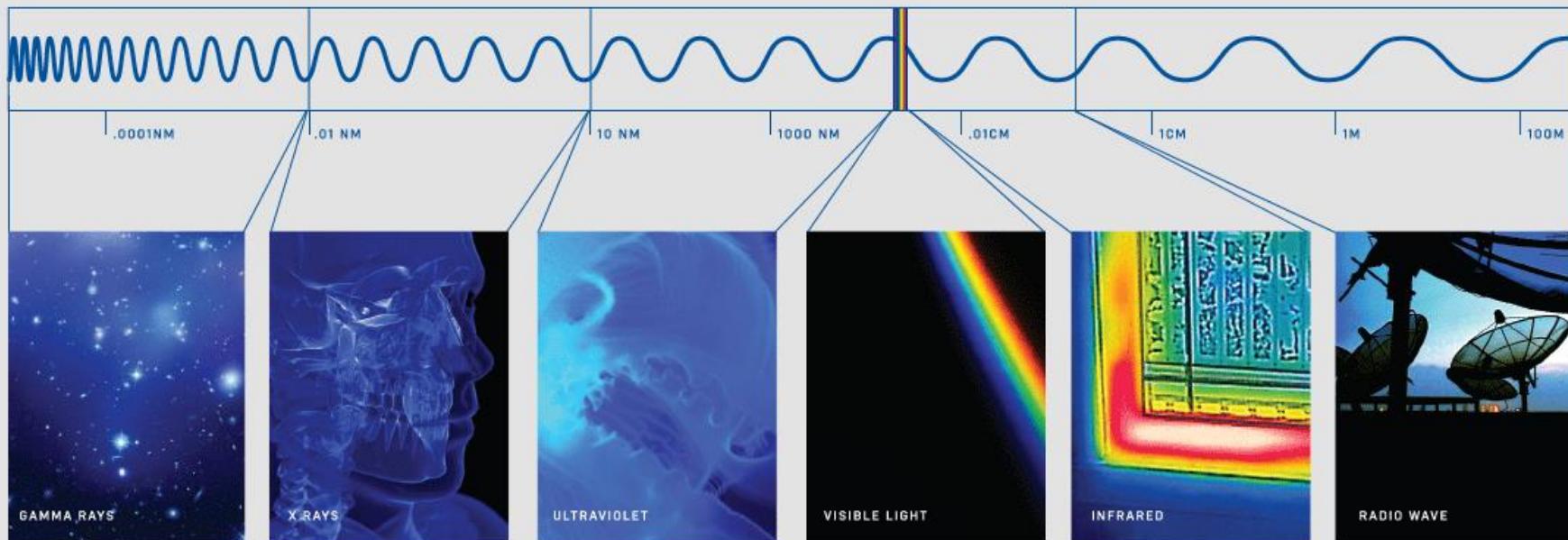


\$28,595.00

Dzokhar Tsarnaev, April 19, 2013
Massachusetts State Police Photo

WHAT IS THERMAL IMAGING

The Electromagnetic Spectrum



Thermal imaging is one of the most powerful technologies ever developed to enhance human vision.

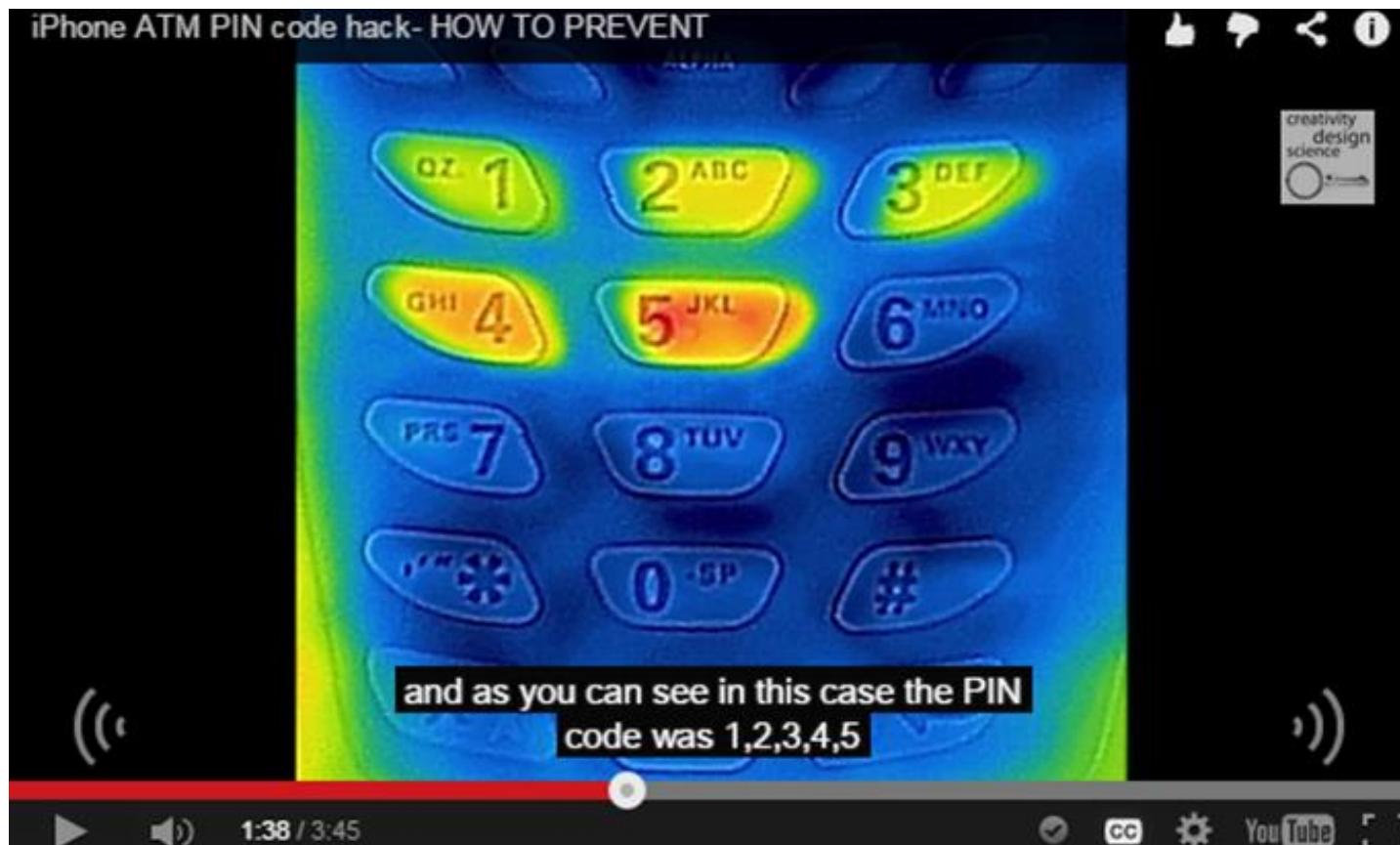
Normally, our vision is limited to a very small portion of the electromagnetic spectrum. Thermal energy has a much longer wavelength than visible light. So long, in fact, that the human eye can't even see it, just like we can't see radio waves.

With thermal imaging, the portion of the spectrum we perceive is dramatically expanded, helping us "see" heat. Visible light doesn't affect the thermal world, so you can see equally well in highly lit and totally dark environments.

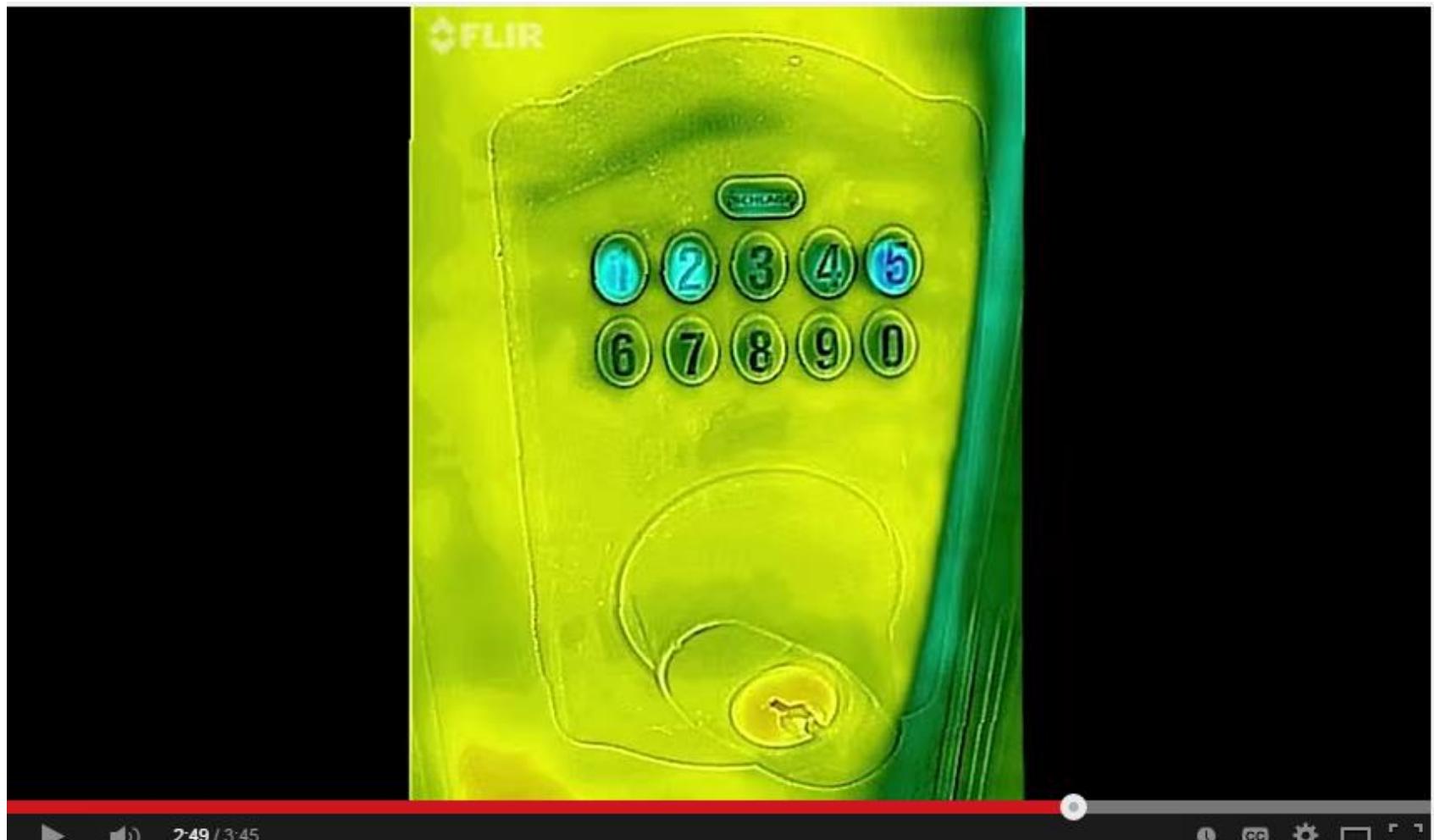


www.flir.com

This quickly lead to Thermal Image PIN Hacking



THEY'D HAVE TO STEAL MY CARD... RIGHT?





HEAT Score



Max: 92 : Min: 22

Waste Heat Information (Gas): Wildwood

Score Distribution



Based on natural gas use, we estimate that **1,020** homes heat an area of **19.13x10⁵ sq.ft** and emit **7,395T** of CO₂e per year at a cost of **\$1,252,276**. By following HEAT recommendations, we estimate total community savings per year of **\$111,188** and a reduction of **657T** of CO₂e per year.

Communities by HEAT Score ▾

15. Arbour Lake	62
16. Rossclair	61
17. Wildwood	52
18. Hawkwood	47
19. Ranchlands	47
20. Parkdale	46
21. Montgomery	46
22. Spruce Cliff	46
23. Scenic Acres	45
24. Silver Springs	42
25. Edgemont	36
26. Varsity	34
27. Bowness	34
28. Brentwood	27
29. Dalhousie	25

Certified HEAT Solutions

Not sure what step to take next? Book a certified home energy audit with **4 Elements**.

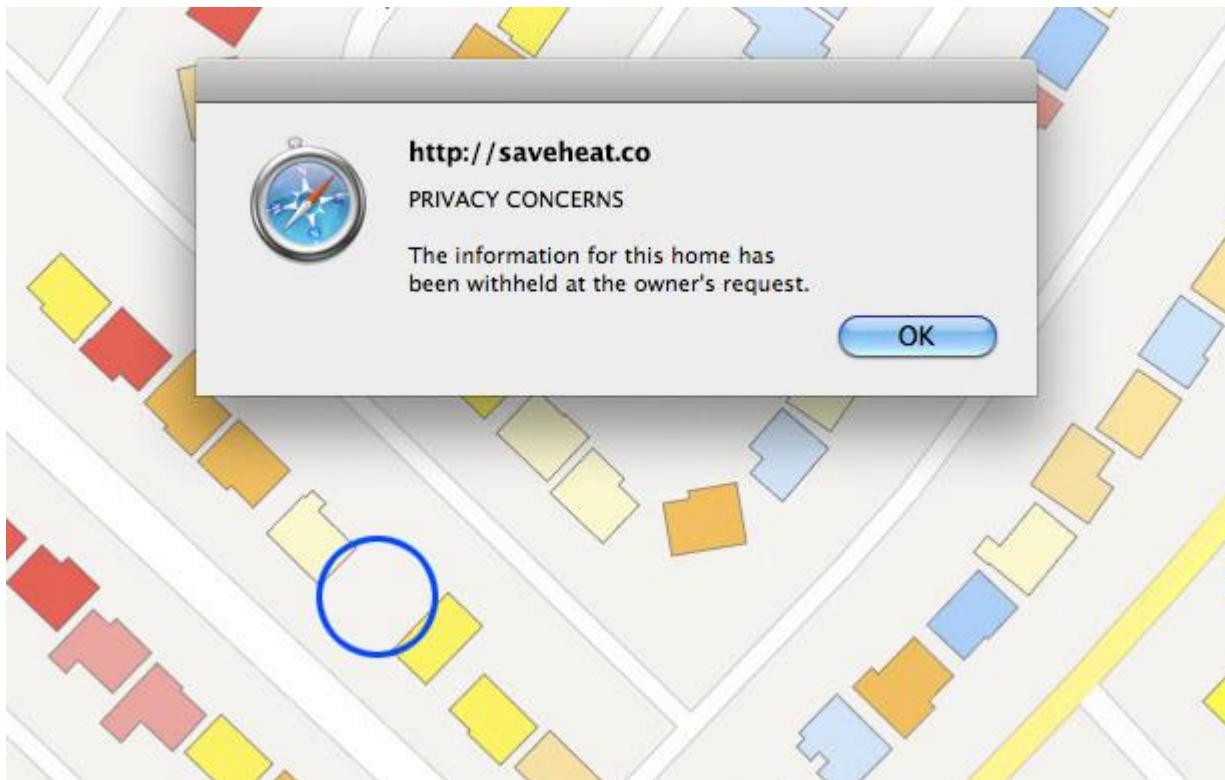


Keep Your Heat In

For further information, check out [this guide](#) by Natural Resources Canada's Office of Energy Efficiency.



WHAT IF I'M CONCERNED ABOUT MY PRIVACY?





Commercial marijuana grow op
Maple Ridge, BC
Source: RCMP Handout photo

THE LEGAL SIDE OF THERMAL IMAGING

Disclaimer: IANAL/IANYL

Kyllo v. United States, 533 U.S. 27 (2001), held that the use of a thermal imaging device from a public vantage point to monitor the radiation of heat from a person's home was a "search" within the meaning of the Fourth Amendment, and thus required a warrant.

Source: Wikipedia

Canada: Section 8 of the Charter

WHAT HAS THIS GOT TO DO WITH BIOMETRICS? -- IT'S ABOUT HOW TECHNOLOGY CAN DRIVE CHANGE

- In *Technocreep*, I predicted that the day will come when you go into a store, enter your PIN, and the pad is swept away like one of these things:

Sensor operated automatic cleaning
EyegieneToilet Seats
Ultra Modern-Non Touch-Pristine Clean



Source: bluelinehygenics.com

THEN WHAT?



Source: biowake.com

AND THEN...

Whoever has access to your DNA has information on your:

- Ancestry
- Genetic predispositions to certain diseases (via single nucleotide polymorphisms and frank abnormalities like trisomy)
- Epigenetics (non-heritable changes such as DNA Methylation)
- AND INFORMATION ON YOUR SIBLINGS AND OTHER GENETICALLY RELATED FAMILY MEMBERS!



Source: appellatesquawk.wordpress.com



SHOULD YOU CARE? WELL, SOMEBODY DOES



Source: www.health-street.net

Jan, 6, 2015:
Genentech Announces
Partnership with
23andMe

Anonymous sperm donor traced on internet

New Scientist, 03 November 2005
ALISON MOTLUK

LATE last year, a 15-year-old boy rubbed a swab along the inside of his cheek, popped it into a vial and sent it off to an online genealogy DNA-testing service. But unlike most people who contact the service, he was not interested in sketching the far reaches of his family tree. His mother had conceived using donor sperm and he wanted to track down his genetic father.

That the boy succeeded using only the DNA test, genealogical records and some internet searches has huge implications for the hundreds of thousands of people who were conceived using donor sperm. With the explosion of information about genetic inheritance, any man who has donated sperm could potentially be found by his biological offspring. Absent and unknown fathers will also become easier to trace.

Source: www.motluk.com

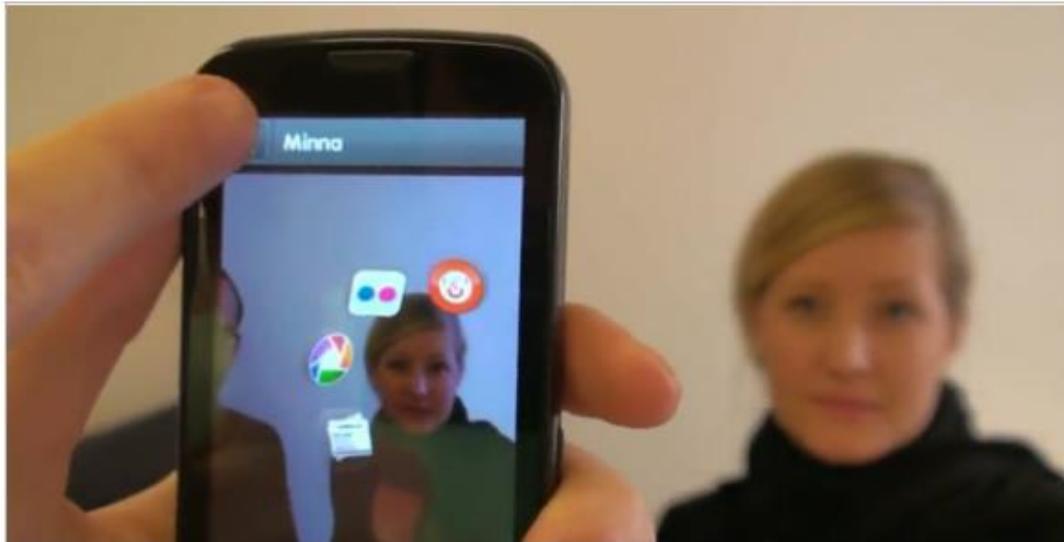
HIDDEN RISK #3: BIOMETRIC DATA'S IRREVERSIBILITY AND THE IMPLICATIONS

- For biometrics such as your DNA cheek swab, it is usually infeasible to withdraw access, once granted.
- Even if taking a sample/hash of a physical feature (features on a fingerprint, selected SNPs of the DNA) there is always the danger of “data jigsawing”
- Legal protection of biometric data is highly variable by jurisdiction
- If credit card numbers are dynamite to have in your possession, DNA data is nuclear fuel!

NEWEST VULNERABILITY: YOUR FACE!

Black Hat: Facial recognition software can link your face to your social security number

Aug. 3, 2011 (1:35 pm) By: Jennifer Bergen



The annual Black Hat security conference is in full swing right now in Las Vegas. The conference, which started on July 30 and goes to August 4, is the place to be for security researchers to discuss and learn about different types of security vulnerabilities seen in almost every area of technology. One area of security that touches close to home for everyone is the privacy of our personal data being linked to our faces. Specifically, information can be linked to your face and made available to anyone who snaps your picture with their smartphone camera.

With major companies like Apple offering face detection APIs to developers in iOS 5, the method of taking a picture and having a database recognize the person's face is available, and over the years, it will only get more and more advanced.

NAMETAG APP



EVEN HOW WE WALK IS BEING STUDIED



“Human gaits, for example, can provide a lot of information about people’s intentions. At the American Army’s Aberdeen Proving Ground in Maryland, a team of gait analysts and psychologists led by Frank Morelli study video, much of it conveniently posted on the internet by insurgents in Afghanistan and Iraq.”

-The Economist, Oct. 2008

HIDDEN RISK #4: OUR BIOMETRICS CAN BE GRABBED WITHOUT OUR CONSENT

- In a public place, and even some “private” spaces, we are exposed
- Face
- Gait
- Speech
- Behavior

New surveillance cameras will use computer eyes to find 'pre crimes' by detecting suspicious behaviour and calling for guards

- Computerised detectors look for 'abnormal' behaviour
- When suspicious individuals are seen, guards called
- BRS machines have been trialled in numerous locations
- 288 cameras to be installed on subway in San Francisco

By ROB WAUGH

PUBLISHED: 13:12 GMT, 5 June 2012 | UPDATED: 13:12 GMT, 5 June 2012

[Comments \(24\)](#) | [Share](#)  26 | [Tweet](#)  191 | [Like](#)  3.5k

A new generation of computerised 'Big Brother' cameras are able to spot if you are a terrorist or a criminal - before you even commit a crime.

The devices are installed in places like train stations or public buildings where they scan passers by to see if they are acting suspiciously.

Using a range of in-built parameters of what is 'normal' the cameras then send a text message to a human guard to issue an alert - or call them.



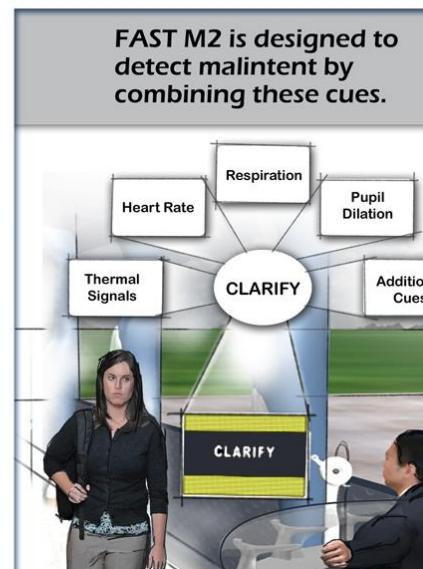
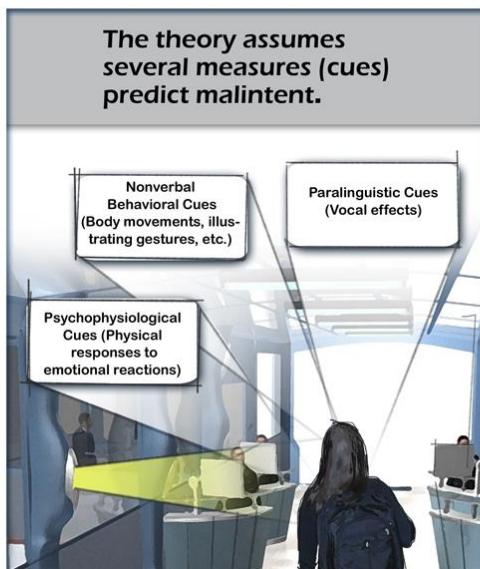
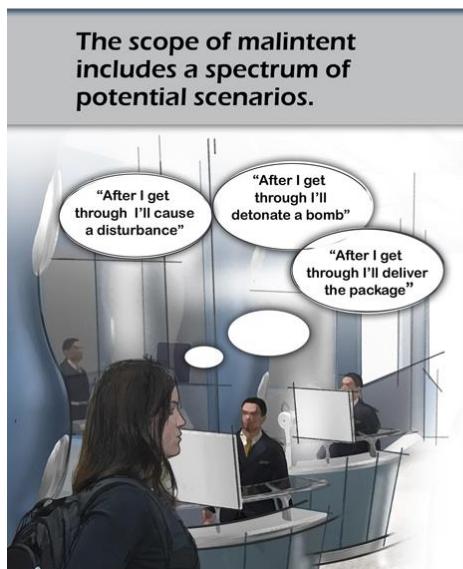
Creepy talking (and listening) surveillance cameras are here

5/15/2012

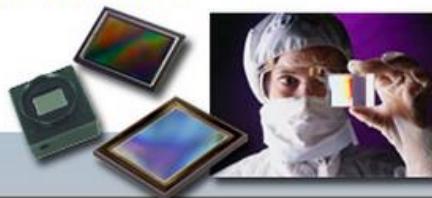
Tricked out street lights incorporating "homeland security applications" that can bark orders at passers-by are being installed in major U.S cities. While this could make your next excursion into the city streets much more exciting, critics are warning the "IntelliStreets system" is a Big Brother step too far. The system includes a variety of cameras and sensors, and perhaps more worryingly, can record conversations. IntelliStreets connects via Wi-Fi and is currently being rolled out in Detroit, Chicago and Pittsburgh, with manufacturers saying it's also suitable for "retail malls, sports venues, on college campuses, and in new construction."

HIDDEN RISK #5: OUR BEHAVIOR CAN RAT US OUT – SOMETIMES INCORRECTLY

- DHS FAST system -- ridiculed at DEFCON 19 (2011) by teenagers



Source: Wikipedia.org which says “Department of Homeland Security, Science and Technology Department - [Sharkride.com](#) but apparently ultimately from a now down DHS website” (unable to authenticate)



3D BIOMETRIC IMAGING

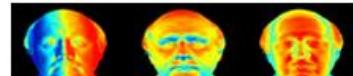
Biometric Imaging

Biometrics

Methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits.

Biometrics comprises methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. Biometric recognition enabled systems are used as a form of secure identity access management and access control. It is also used to identify individuals in groups that are under surveillance.

Standoff Biometrics is the ability to collect biometric data, overtly or covertly, from a distance.



Biometric characteristics can be divided in two main classes:

Physiological Biometrics are related to the shape of the body. Examples include, but are not limited to facial and iris recognition, hand - palm geometry and fingerprints.

Behaviometrics are related to the behavior of a person. Examples include, but are not limited to body posture movement, gait and micro-expressions.

[Click Here For Demo Video](#)

3D Biometric Sensors

Photon-X 3D Volumetric Sensors

At the core of Photon-X 3D technologies are a series of patented SPI Biometric Sensors. These innovative sensors [...] [More..](#)

Photon-X 3D biometric sensors can be integrated with existing video surveillance systems, adding a powerful combination of 3D biometric capture, along with motion and shape analysis capabilities.



The multi-modal (full range) set of biometrics such as facial recognition, iris scanning, fingerprint/full case prints, micro-gestures, full body motion and gait detection can be isolated and analyzed in milliseconds allowing for faster identification and reaction times.

System Capabilities

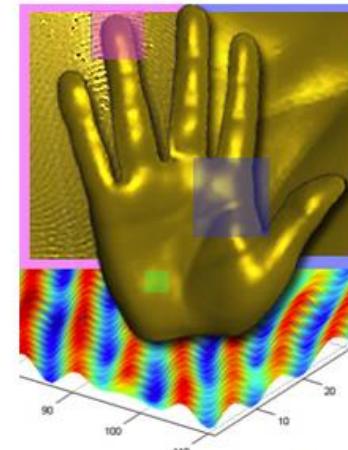
- * Innovative standof biometric capture
- * Supports full range of biometric modalities

3D Biometric Applications

Photon-X 3D Volumetric Applications

Standoff Biometric imaging sensors to support a wide range of applications and markets.

Finger Prints Palm Prints



[Click Here For Demo Video](#)

Standoff Automatic Fingerprint Extraction

Source: www.photon-x.com
© 2010 Photon-X

GOOD MEMORIES, BAD MEMORIES, FALSE MEMORIES COURTESY OF



Solicitation Number: DARPA-BAA-12-03 **Notice Type:** Presolicitation

Synopsis:

Added: Oct 07, 2011 1:11 pm

DARPA is soliciting innovative research proposals in the areas of (1) quantitative analysis of narratives, (2) understanding the effects narratives have on human psychology and its affiliated neurobiology, and (3) modeling, simulating, and sensing-especially in stand-off modalities-these narrative influences. Proposers to this effort will be expected to revolutionize the study of narratives and narrative influence by advancing narrative analysis and neuroscience so as to create new narrative influence sensors, doubling status quo capacity to forecast narrative influence.

RISK #6: GIVING OUR BIOMETRIC AND BEHAVIORAL DATA MAY BE (*DE FACTO*) MANDATORY

- In India, biometric ID is legally mandated and needed to obtain government services.
- You can rent a car without a credit card (but just try to!)
- You can also ask for a paper ticket at a Disney theme park instead of this:



Source: findingmickey.com

DRIVER TRACKING APPS ARE JUST THE START...

CNN Money

Business Markets Tech Personal Finance Small Business Luxury

stock tickers



Would you wear a tracker to get an insurance discount?



By Jose Pagliery @Jose_Pagliery



John Hancock will let you wear a Fitbit -- and share all its data -- for cheaper life insurance.

Most Popular



California: The
nation's most
unequal state



2 ways to get
guaranteed
retirement income



Premarkets: 4 things
to know before the
open

For the first time ever in the United States, a life insurance company is offering a discount -- if you're willing to let it track your health, location and body.

Source: cnn.com

Your Fuelband Knows When You're Having Sex



Adam Clark Estes

Filed to: SEX 7/12/13 12:42pm

109,375



4



Source: gizmodo.com

Everybody loves these Fuelbands and other activity trackers because they supply you with troves of data about your everyday life. Sometimes, however, it's a little bit too much information.

Your fitness wristband knows when you're having sex. If it's sensitive enough to detect minute movements while you're sleeping, it can certainly pick up on the patterns of intercourse. Plus how else do you explain getting a half hour of exercise late at night without taking a single step.

WORKPLACE ISSUES

Companies are giving fitness monitors and other wearable to employees as part of fitness programs

“Four out of five employees would use company-provided wearable that tracks health and wellness and provide that data to their employer.”

(<http://www.cornerstoneondemand.com/SOWP14>)

Perks might include discounts on fitness programs, extra vacations days, a bonus

BUT... Did you get a good night's sleep? Or...



Source: Licensed from Colourbox



HIDDEN RISK #7: BIOMETRIC DATA THIEVES AND AGGREGATORS

- Like any other data, biometric data is subject to breach, hacking, being held for ransom
- “Bits is bits” so why wouldn’t companies Acxiom (and Google) try to grab biometric data (if they are allowed to)
- Well the good news is that there is, at least, some awareness of the ethical issues:

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.

A FRAMEWORK FOR MAKING ALL THIS “NEWS YOU CAN USE”

Even before you get back to the office, list technologies that you use or are considering using that have biometric components

Apply this “creepy lens” to identify ways in which it might upset people or compromise their privacy or confidence

Think about alternatives that will produce “pretty good information” A sign-in sheet at the company gym will track attendance, if not effort, as well as a fitness band. What do you really need to collect?

LONGER TERM APPLICATION OF WHAT YOU HAVE LEARNED TODAY

Check your data retention policies (example: videotapes should usually be erased after 7 days if not requested)

Consider whether some data should be de-identified (which can be difficult!) or collected anonymously or not at all

View every new technology through the creepy lens and make sure the benefits outweigh the risks

Don't Be Creepy!

THANK YOU!

Tom Keenan, FCIPS, I.S.P.

keenan@ucalgary.ca

@drfuture

<http://www.psychologytoday.com/blog>

/technocreep

www.technocreep.com

