

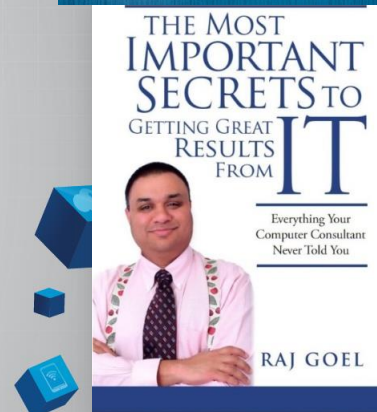
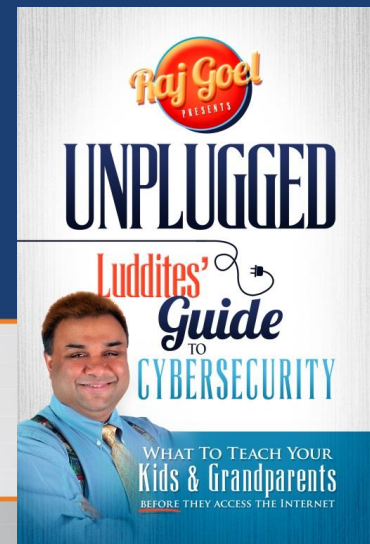
# PANOPTICON 2015: Continued Erosion Of Privacy Rights (and Occasional Victories)

Raj Goel, CISSP

raj@brainlink.com / 917-685-7731

www.RajGoel.com

@rajgoel\_ny



# Media Appearances



Global Business and Technology Association™



The New York Times

Entrepreneur

(ISC)<sup>2</sup>

SECURITY TRANSCENDS TECHNOLOGY™

BrightTALK™



PenTest magazine



NEW YORK COUNTY  
NYCLA  
LAWYERS' ASSOCIATION

# Raj Goel, CISSP

- » Author, entrepreneur, IT expert and public speaker, Raj Goel is globally known as the go-to man in cyber security and privacy law. He is committed to educating individuals and organizations about online safety and how to protect their most important assets – **people and data**. His expert advice helps individuals, companies and conglomerates navigate their way through the world's ever-changing technology and increasingly complex IT compliance laws. He often appears in the media and at conferences world-wide to educate the public on cyber-security and digital privacy, a subject he is passionate about.

## Security, Civil Liberties and Peace of Mind

- » When you need the right approach to complying with HIPAA/HITECH, PCI-DSS or simply protecting your assets, Raj Goel, as any of his loyal clients will tell you, is the man to call upon. Raj's credentials are impeccable. A 25-year veteran of the IT industry and an expert in online security, Raj has personally consulted with organizations ranging from Fortune 100 corporations to small family companies to governments world wide.
- » Raj is fueled by his passion for enhancing Civil Rights in Cyberspace, his love of helping people keep themselves, their families and their companies safe online. He is available as a consultant and a public speaker and often sought after by major media outlets and companies.

## Key highlights:

- **Author**, "UNPLUGGED Luddites Guide To Cybersecurity", Amazon, 2015
- **Author**, "The Most Important Secrets To Getting Great Results From IT", Amazon, 2012
- **On-Air Television Cybersecurity Expert**, WPIX11, New York City (2013-present)
- **On-Air Cybersecurity Expert**, Columbia News Tonight, Columbia University, NYC
- **Keynote speaker**, NCSL 2013, Government of Netherlands, The Hague, Netherlands
- **Keynote speaker**, Government Of Curacao, 2013
- **Keynote speaker**, "what should MSP's know about compliance", Datto partner conference, 2013
- **Author**, "Googling Your Privacy and Security Away", Infosecurity Professional Magazine
- **Author**, "Trends In Financial Crimes", Infosecurity Professional Magazine
- **Author**, "Life Of A Child (2014) – raising a generation of cyber-at-risk youth", Infosecurity Professional Magazine, 2014
- **Author**, "Welcome To The World Of Dating Sites", Infosecurity Professional Magazine, 2015

# Who I keep getting confused with



- » Not Javvad Malik
- » Not a handsome duckface
- » No British Accent

# PRISM – How & What

How can we monitor everything?

Most of the world's communications are flowing through the U.S.

So is your targets' data.



Email



Chat



Videos



Photos



File Transfers



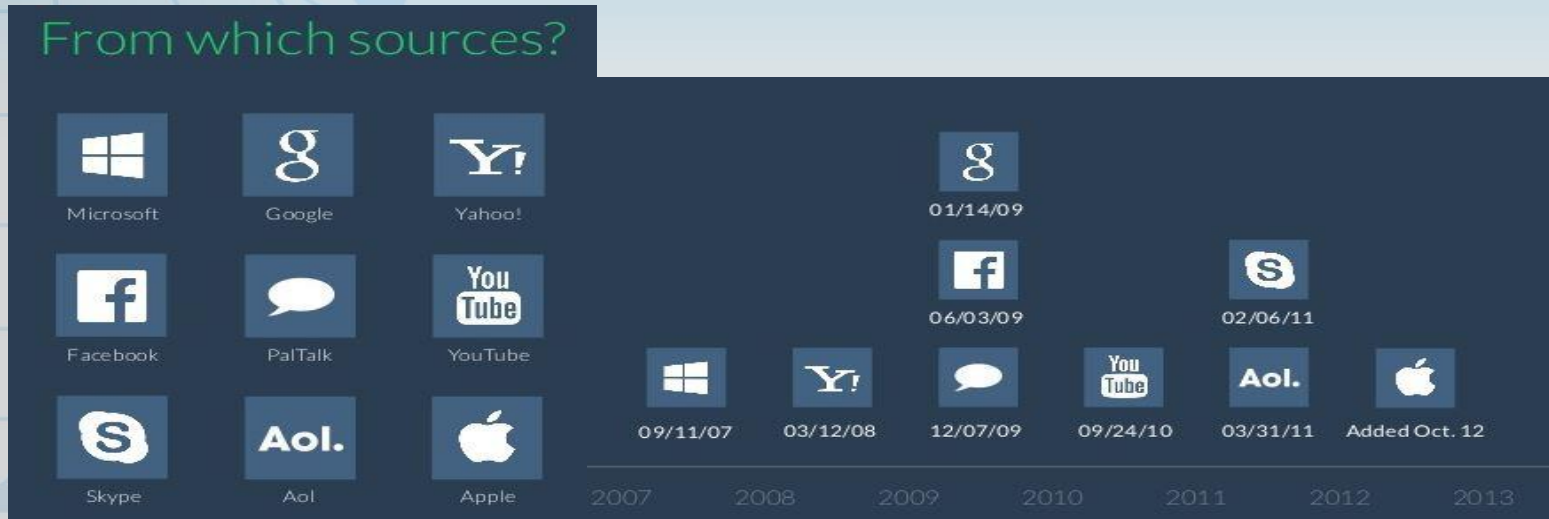
Login Activity



Social Media Profiles

<http://fr.slideshare.net/EmilandDC/dear-nsa-let-me-take-care-ou>

# PRISM – The Players



<http://fr.slideshare.net/EmilandDC/dear-nsa-let-me-take-care-ou>

# UK: GCHQ Karma Police

- » GCHQ's mass-surveillance activities have detailed an operation codenamed KARMA POLICE, which slurped up the details of "every visible user on the Internet".
- » The operation was launched in 2009, without Parliamentary consultation or public scrutiny, to record the browsing habits of "every visible user on the Internet" without the agency obtaining legal permission to do so, according to documents published by *The Intercept*.
- » KARMA POLICE was constructed between 2007 and 2008, and [according to slides](#) was developed with the explicit intention of correlating "every user visible to passive SIGINT with every website they visit, hence providing either (a) a web browsing profile for every visible user on the Internet, or (b) a user profile for every visible website on the Internet."
- » [http://www.theregister.co.uk/2015/09/25/gchq\\_tracked\\_web\\_browsing\\_habits\\_karma\\_police/](http://www.theregister.co.uk/2015/09/25/gchq_tracked_web_browsing_habits_karma_police/)

# Germany: BND + NSA = Stasi 2

- » BND — may have separately aided U.S. agents with snooping on hundreds of European companies, regional entities and politicians. The targets, according to a report in the German newspaper Süddeutsche Zeitung on Thursday, included French and European Commission officials.
- » The new disclosures center on a list of 2,000 suspicious “selectors” — including phone numbers, IP addresses and e-mails — provided by the United States and plugged into German intelligence data systems that the Germans later determined exceeded the operation’s mandate
- » [https://www.washingtonpost.com/world/europe/nsa-scandal-rekindles-in-germany-with-an-ironic-twist/2015/04/30/030ec9e0-ee7e-11e4-8050-839e9234b303\\_story.html](https://www.washingtonpost.com/world/europe/nsa-scandal-rekindles-in-germany-with-an-ironic-twist/2015/04/30/030ec9e0-ee7e-11e4-8050-839e9234b303_story.html)



# FBI, Next Gen Ident (NGI)

- » **FBI Plans to Have 52 Million Photos in its NGI Face Recognition Database by Next Year**
- » NGI builds on the FBI's legacy fingerprint database—which already contains well over 100 million individual records—and has been designed to include multiple forms of biometric data, including palm prints and iris scans in addition to fingerprints and face recognition data. NGI combines all of these forms of data in each individual's file, linking them to personal and biographic data like name, home address, ID number, immigration status, age, race, etc. This immense database is shared with other federal agencies and with the approximately 18,000 tribal, state and local law enforcement agencies across the United States.

<https://www.eff.org/deeplinks/2014/04/fbi-plans-have-52-million-photos-its-ngi-face-recognition-database-next-year>

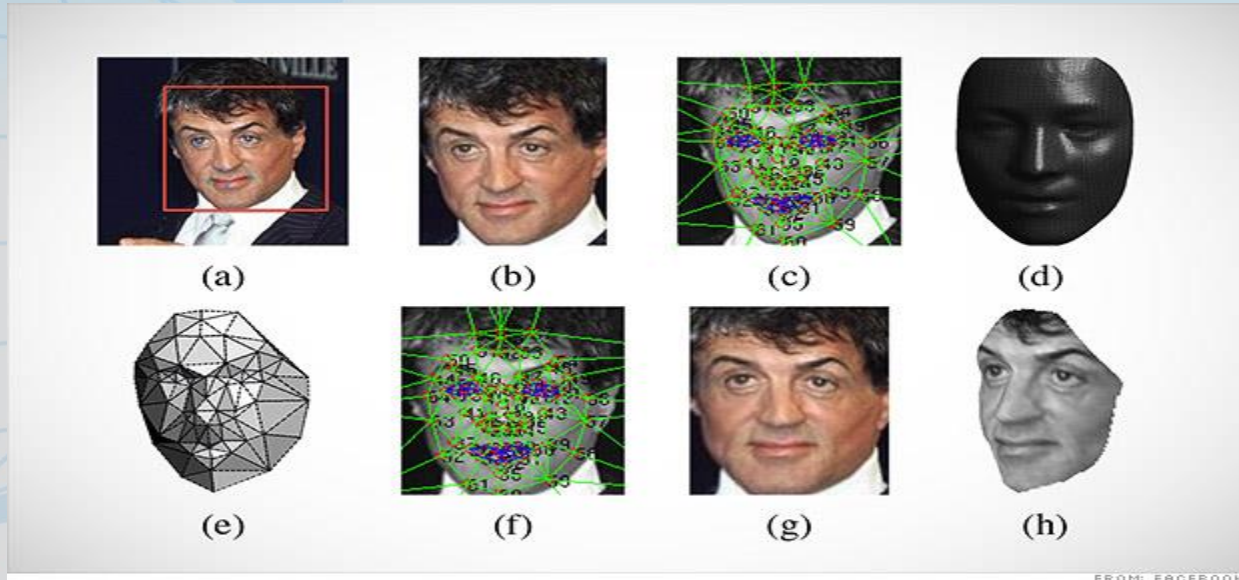
# 100x Better, 1M Faster, Dirt Cheap

- » As Lesley Stahl reported on "60 Minutes", "the ability of computers to identify faces has gotten 100 times better, a million times faster, and exponentially cheaper."
- » The "60 Minutes" segment gives an in-depth account of all the scary advancements in the field – highlighting the technology's ability to track your whereabouts, mine your personal data, and even predict your social security number.

<http://www.businessinsider.com/advertisers-using-facial-recognition-technology-2013-5>



# Facebook Side Profiling



<http://money.cnn.com/2014/04/04/technology/innovation/facebook-facial-recognition/>

# What Does Facebook Sell About You To Corporations, Governments, etc.?

**Facebook Gender**

Get access to the following for users that authenticate with Facebook:

**Basic Profile** Enterprise Pro Plus Basic  
Read access to the users' profile data. Returned by the `auth_info` API call.

Address	Birthday	Email	Profile Photo
Verified Email	Display Name	Gender	Homepage
Identifier	Name	Preferred Username	UTC Offset

**Extended Profile** Enterprise Pro Plus  
Read access to the users' extended profile data. Returned by the `auth_info` API call.

About Me	Activities	Addresses	Albums
Books	Current Location	Emails	Games
Groups	Interested In M...	Interests	Languages Spoken
Movies	Music	Organizations	Page Likes
Photos	Political Views	Quotes	Relationship St...
Religion	Status	TV Shows	Videos
Friends List	Heroes	Id	Last Updated
Name	Profile URL	Sports	URLs

**Contacts** Enterprise Pro  
Read access to the users' friends. Returned by the `get_contacts` API call.

About Me	Activities	Addresses	Birthday
Books	Current Location	Interested In M...	Interests
Languages Spoken	Movies	Music	Organizations
Photos	Political Views	Quotes	Relationship St...
Religion	Status	TV Shows	Display Name
Gender	Heroes	Id	Last Updated
Name	Preferred Username	Profile URL	Sports
URLs			

<https://twitter.com/TheBakeryLDN/status/427531934294880256/photo/1>

# Computers Beat Humans

- » **The Face Recognition Algorithm That Finally Outperforms Humans**
- » **Computer scientists have developed the first algorithm that recognizes people's faces better than you do**
- » Humans: 97.53%
- » Machine: 98.52%

<https://medium.com/the-physics-arxiv-blog/2c567adbf7fc>

# Minority Report



- » Technology giant NEC's Hong Kong branch is promoting a small, "easy to install" appliance which will enable businesses to monitor their customers based on facial recognition.
- » From a recent NEC press release:  
The new Mobile Facial Recognition Appliance enables organizations in any industry to offer an ultra-personalized customer experience by recognizing the face of each and every customer as soon as they set foot on the premises.

<http://nakedsecurity.sophos.com/2014/04/21/facial-recognition-coming-soon-to-a-shopping-mall-near-you/>



# You!

## TARGET

- » Target has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start buying diapers.
- » Lots of people buy lotion, but one of Pole's colleagues noticed that women on the baby registry were buying larger quantities of unscented lotion around the beginning of their second trimester. Another analyst noted that sometime in the first 20 weeks, pregnant women loaded up on supplements like calcium, magnesium and zinc. Many shoppers purchase soap and cotton balls, but when someone suddenly starts buying lots of scent-free soap and extra-big bags of cotton balls, in addition to hand sanitizers and washcloths, it signals they could be getting close to their delivery date.

<http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>

# Disney + NSA



- » Eric Haseltine left his post as executive vice president of research and development at Walt Disney Imagineering in 2002 to become associate director for research at the NSA and then became National Intelligence Director John Negroponte's assistant director for science and technology.
- » Bran Ferren, who served on advisory boards for the Senate Intelligence Committee and offered his technological expertise to the NSA and the DHS.
- » Mickey does it at "the most wonderful place on Earth" – and willingly shares his biometrics secrets with the government

Read more: <http://www.businessinsider.com/this-is-how-we-know-that-the-shocking-revelations-about-trapwire-spying-are-true-2012-8#ixzz3GyZqGHk3>





# Babies & Children 0-10

## BABIES



### Star Wars Clothes & Toys:

You know you still have your Empire Strikes Back bedsheets.



**Pixar** includes the names of any crew member's babies in the credits who were born during the production of the movie, called "Poduction Babies."

**Disney Channel** #1 for kids in 2012, topping Nickelodeon's 17-year record.



**Disney** acquires the Muppets intellectual property rights - but does not own the rights to *Fraggle Rock* or *Sesame Street*



### Star Wars Movies:

Let's face it - if you're alive on planet earth at any age, you're going to see one of these films.

## CHILDREN



Who says athletes aren't smart? ESPN broadcasts the National Spelling Bee

Star Wars: *The Clone Wars*

Star Wars Legos

Star Wars Toys



Disney really scored by taking *The Avengers* under its wing. *The Avengers* film was the highest grossing Marvel Comics film to date.

**Pixar Child Development Center** (for Pixar employees children only)

*Toy Story 3* is the first animated film to make over \$1 billion worldwide.

1,000,000,000

While Disney has cornered the princess market, their acquisition of Marvel Comics ensures that they've got a pretty good position on the superhero market as well.



**Marvel TV:** *Ultimate Spiderman* on Disney XD



# MagicBands of Surveillance



A crucial part of the system: “MagicBands” - bracelets equipped with Radio Frequency Identification (RFID) chips that “will function as room key, park ticket, FastPass and credit card.”

Did you buy a balloon? What attractions did you ride and when? Did you shake Goofy's hand, but snub Snow White? If you fully use MyMagic+, databases will be watching, allowing Disney to refine its offerings and customize its marketing messages.

<http://www.alternet.org/disneys-creepy-new-surveillance-tool>

# Weddings



It's New York City's Bridal Fashion Week, and Disney Weddings staged a beautiful fashion show for the 2015 Disney's Fairy Tale Weddings by Alfred Angelo collection. The highlight of the show was the revealing of the brand new Elsa-inspired wedding dress.

<http://blogs.disney.com/disney-style/fashion/2014/10/09/the-elsa-inspired-wedding-gown-is-here/>

# KGB vs Disney

After executing family members, the KGB used to send a bill for the bullet.

Today, we pay [Disney, Amazon, Apple, Verizon, Google, etc] bills that subsidize our own surveillance.

# SEC, DOJ, ECPA

- » For a long time, the **Department of Justice DOJ** argued **ECPA allowed it to circumvent the Fourth Amendment and access much of your email without a warrant.**
- » **Securities and Exchange Commission (SEC)**, may be doing the same exact thing: **it is trying to use ECPA to force service providers to hand over email without a warrant, in direct violation of the Fourth Amendment.**
- » ECPA has been used to argue that emails older than 180 days may be accessed without a warrant based on probable cause. Instead, the agencies send a mere subpoena, which means that the agency does not have to involve a judge or show that the emails will provide evidence of a crime.

<https://www.eff.org/deeplinks/2014/04/sec-obtaining-emails-without-warrant-or-not>

# Utah Cops, Warrantless Search

- » Utah law enforcement officials searched, **without a warrant, the prescription drug records of 480 public paramedics, firefighters and other personnel to try to figure out who was stealing morphine from emergency vehicles.**
- » **The warrantless search of Utah's database chronicling every controlled substance dispensed by a pharmacist resulted in charges against one paramedic that have nothing to do with the original investigation.** Instead, the authorities discovered an employee whose records exhibited "the appearance of Opioid dependence" and lodged prescription fraud charges against paramedic Ryan Pyle. Now Pyle faces a maximum five-year prison sentence if convicted of the felony.

<http://arstechnica.com/tech-policy/2014/04/utah-cops-warrantlessly-search-drug-records-of-480-emergency-personnel/>

# Police in North Dakota can now use drones armed with tasers

- » Police in North Dakota are now authorized to use drones armed with tasers, tear gas, rubber bullets, and other "non-lethal" weapons, following the passage of Bill 1328.
- » Sponsored by Rep. Rick Becker (R-Bismarck), the bill was originally intended to limit the police's surveillance powers, and banned all weapons on law enforcement drones. Then a policy lobby group was allowed to amend the bill, though, at which point it only banned lethal weapons, writes *The Daily Beast*.  
<http://www.theverge.com/2015/8/26/9211165/north-dakota-armed-drones-tasers>
- » How soon until these drones get hacked?



# Samsung smart fridge leaves Gmail logins open to attack

- » Pen Test Partners discovered the MiTM (man-in-the-middle) vulnerability that facilitated the exploit during an IoT hacking challenge at the recent DEF CON hacking conference.
- » The hack was pulled off against the RF28HMELBSR smart fridge, part of Samsung's line-up of Smart Home appliances which can be controlled via their Smart Home app. While the fridge implements SSL, it fails to validate SSL certificates, thereby enabling man-in-the-middle attacks against most connections.
- » The internet-connected device is designed to download Gmail Calendar information to an on-screen display. Security shortcomings mean that hackers who manage to jump on to the same network can potentially steal Google login credentials from their neighbours.
- » "The internet-connected fridge is designed to display Gmail Calendar information on its display," explained Ken Munro, a security researcher at Pen Test Partners. "It appears to work the same way that any device running a Gmail calendar does. A logged-in user/owner of the calendar makes updates and those changes are then seen on any device that a user can view the calendar on."
- » "While SSL is in place, the fridge fails to validate the certificate. Hence, hackers who manage to access the network that the fridge is on (perhaps through a de-authentication and fake Wi-Fi access point attack) can Man-In-The-Middle the fridge calendar client and steal Google login credentials from their neighbours, for example."

[http://www.theregister.co.uk/2015/08/24/smart\\_fridge\\_security\\_fubar/](http://www.theregister.co.uk/2015/08/24/smart_fridge_security_fubar/)

# Police secretly track cellphones to solve routine crimes

- » BALTIMORE — The crime itself was ordinary: Someone smashed the back window of a parked car one evening and ran off with a cellphone. What was unusual was how the police hunted the thief.
- » Detectives did it by secretly using one of the government's most powerful phone surveillance tools — capable of intercepting data from hundreds of people's cellphones at a time — to track the phone, and with it their suspect, to the doorway of a public housing complex. They used it to search for a car thief, too. And a woman who made a string of harassing phone calls.
- » In one case after another, USA TODAY found police in Baltimore and other cities used the phone tracker, commonly known as a stingray, to locate the perpetrators of routine street crimes and frequently concealed that fact from the suspects, their lawyers and even judges. In the process, they quietly transformed a form of surveillance billed as a tool to hunt terrorists and kidnappers into a staple of everyday policing.
- » The suitcase-size tracking systems, which can cost as much as \$400,000, allow the police to pinpoint a phone's location within a few yards by posing as a cell tower. In the process, they can intercept information from the phones of nearly everyone else who happens to be nearby, including innocent bystanders. They do not intercept the content of any communications.

<http://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/>

# NC Law: Teens who take nude selfie photos face adult sex charges

- » After a 16-year-old Fayetteville girl made a sexually explicit nude photo of herself for her boyfriend last fall, the Cumberland County Sheriff's Office concluded that she committed two felony sex crimes against herself and arrested her in February.
- » The girl was listed on a warrant as both the adult perpetrator and the minor victim of two counts of sexual exploitation of minor - second-degree exploitation for making her photo and third-degree exploitation for having her photo in her possession.
- » Psychologist Jeff Temple of the University of Texas Medical Branch said his research has found that **28 percent of teens use their cellphones to send naked photos of themselves to other teens**
- » Although the pictures are illegal, **sexual intercourse between 16-year-old teens is not**. The **age of consent for sexual activity in North Carolina is 16**, and it dips younger than that for **teens who are less than four years apart in age**.

[http://www.fayobserver.com/news/local/nc-law-teens-who-take-nude-selfie-photos-face-adult/article\\_ce750e51-d9ae-54ac-8141-8bc29571697a.html](http://www.fayobserver.com/news/local/nc-law-teens-who-take-nude-selfie-photos-face-adult/article_ce750e51-d9ae-54ac-8141-8bc29571697a.html)

# Foreign Spooks Use Hacked US Data to Root Out Spies

- » Intelligence services in China, Russia and elsewhere are capitalizing on a treasure trove of recently hacked US government data to identify American spies, according to a new report.
- » Foreign powers are using data stolen from the Office of Personnel Management (OPM) in particular and combining it with breached information from healthcare providers like Anthem, infidelity site Ashley Madison, United Airlines, and other firms to build up a digital identity for US intelligence operatives.
- » This can then be used to track or even blackmail and recruit US spies, according to the Los Angeles Times.
- » US counter-intelligence boss, William Evanina, claimed that this activity can help identify “who is an intelligence officer, who travels where, when, who’s got financial difficulties, who’s got medical issues, [to] put together a common picture.”
- » He added that foreign powers were “absolutely” using this information to root out US spies, with unnamed officials pointing the finger at China and Russia as prime culprits.

<http://www.infosecurity-magazine.com/news/foreign-spooks-hacked-us-data-root/>

# OPM Breach – 5.6M fingerprints stolen

- » The Office of Personnel Management announced Wednesday that 5.6 million people are now estimated to have had their fingerprint information stolen.
- » That number was originally thought to be about 1.1 million, OPM said in a statement. About 21.5 million individuals had their Social Security Numbers and other sensitive information affected by the hack.
- » According to OPM, "federal experts believe that, as of now, the ability to misuse fingerprint data is limited." The office acknowledged, however, that future technologies could take advantage of this information.

<http://www.cnbc.com/2015/09/23/office-of-personnel-mgmt-56m-estimated-to-have-fingerprints-stolen-in-breach.html>

# Kaspersky – Companies hack their own customers


- » Online advertising and profiling companies harvest users' personal information en masse. Some weeks ago, Kaspersky's Sean Sullivan wrote an interesting piece about browsing trackers, where he showed that an **ordinary IKEA web page will invite a stunning total of 49 trackers** leeching information from the user. These trackers are not limited to IKEA, but instead follow your movements as you continue to browse the net. If you were not tagged by them by then, IKEA just did you a disservice by inviting them all after you. If you are interested in learning more about online profiling, read "The Daily You" by Joseph Turow.
- » Car hacking wasn't invented by Charlie Miller – VW beat them to it
- » Remember the Sony root-kit laden CDs?
- » Ashley Madison never really deleted profiles
- » Lenovo shipped embedded spyware...repeatedly

<https://business.f-secure.com/vulnerabilities-hacking-and-questionable-business-practices/>

**TWEETS  
SINK  
FLEETS**

**THINK OPSEC.**

**CONTACT YOUR FSO IF YOU SUSPECT A SECURITY BREACH.**

 **DEFENSE SECURITY SERVICE**  
*National Security is Our Mission*

[WWW.DSS.MIL](http://WWW.DSS.MIL)

# Priceline, Travelocity, and Cingular fined for using adware

- » **Priceline, Travelocity, and Cingular**, three high-profile companies **that advertised through nuisance adware programs** have agreed to pay fines and reform their practices, according to the New York Attorney General.
- » “Advertisers will now be held responsible when their ads end up on consumers’ computers without full notice and consent,” Andrew Cuomo said. “Advertisers can no longer insulate themselves from liability by turning a blind eye to how their advertisements are delivered, or by placing ads through intermediaries, such as media buyers. New Yorkers have suffered enough with unwanted adware programs and this agreement goes a long way toward clamping down on this odious practice.”
- » PressEsc.com January 29, 2007



# Victory - FBI told 'get a warrant'

- » The US Department of Justice has moved to quell the ongoing row over the use of IMSI-catchers like Stingray, with a new policy that requires a warrant before they're deployed.
- » The policy, announced here, is designed to “establish a higher and more consistent legal standard and increase privacy protections” for the use of cell-site simulators.
- » The policy takes effect immediately and applies across all DoJ agencies.
- » The policy also addresses the understandable fear that anyone's cellphone use could be caught by the devices, merely because they happened to be in the same place at the same time as a Stingray was in use.
- » The DoJ statement notes that the policy “includes data handling requirements and an agency-level implementation of an auditing program to ensure that data is deleted consistent with this policy. For example, when the equipment is used to locate a known cellular device, all data must be deleted as soon as that device is located, and no less than once daily.”
- » The controversial devices have been under attack from the ACLU, and lawyers in the US are working through FBI use of Stingrays in case convictions can be appealed.
- » The new policy has been welcomed by House Oversight and Government Reform Committee Chairman Jason Chaffetz, who released this statement on TwitLonger.
- » “As I've long stated, establishing a high uniform standard helps protect personal privacy and discourages abuse and mishandling of these powerful devices,” he wrote.
- » He states that the battle isn't over, since there's still secrecy around the use of geolocation technology, and Chaffetz says the DoJ should “continue to produce information – including the Jones memos – to help Congress and the public understand how the federal government tracks people.”

[http://www.theregister.co.uk/2015/09/04/stingray\\_stung\\_fbi\\_told\\_get\\_a\\_warrant/](http://www.theregister.co.uk/2015/09/04/stingray_stung_fbi_told_get_a_warrant/)

# Victory - Baltimore lawyers vow to review 2,000 FBI Stingray snoop cases

- » Defense attorneys in Baltimore, US, are planning to reexamine 2,000 police arrests made with the assistance of Stingray – the cellphone surveillance equipment that identifies and logs mobile device owners within range.
- » A group of lawyers including the city's public defender want to get a closer look at whether they can challenge some of the arrests made in part on evidence gathered by the secretive phone-tracking tool.
- » The legal eagles believe the cops' use of the technology was excessive and unconstitutional in some or all cases – and wants any convictions thrown out if necessary.
- » "This is a crisis, and to me it needs to be addressed very quickly," Baltimore public defender Natalie Finegar told USA Today, though Finegar conceded to the Baltimore Sun that "it's going to be a labor-intensive process."

[http://www.theregister.co.uk/2015/08/28/baltimore\\_stingray\\_cases/](http://www.theregister.co.uk/2015/08/28/baltimore_stingray_cases/)

# Victory – Court rules smartphone passwords are protected...

- » The Feds can't make suspects give up their company-issued smartphone passcodes because doing so violates the Fifth Amendment of the US Constitution.
- » So ruled Judge Mark Kearney of the federal court in East Pennsylvania in the case of *Securities and Exchange Commission v Huang*, [an insider-trading case](#) brought against two ex-Capital One bank workers. While that's good news for the defendants, Bonan Huang and Nan Huang, it's very bad news for prosecutors.
- » The Pennsylvania court ruled on Wednesday that forcing the pair to unlock the passcode-protected devices would violate their constitutional rights – specifically the [Fifth Amendment](#), which spells out the right against self-incrimination.
- » "We find, as the SEC is not seeking business records but defendants' personal thought processes, defendants may properly invoke their Fifth Amendment right," the judge wrote in his analysis [[PDF](#)].
- » "Absent waiver of the confidentiality attendant to this personal thought process, we cannot find the personal passcodes to the Bank's smartphones to be corporate records falling under the collective entity cases. We find Defendants' confidential passcodes are personal in nature and Defendants may properly invoke the Fifth Amendment privilege to avoid production of the passcodes."
- » Oddly enough, this wouldn't be an issue if the smartphones in question used a fingerprint access system, rather than a passcode. Last year, a court ruled in Virginia that cops could force a suspect to unlock their phone using a fingerprint, since this is no different from being fingerprinted at a police station or giving a DNA swab.
- » **It's a very fine legal distinction. A passcode is a thought process, which does get Fifth Amendment protection, whereas a biometric identifier is out in the open.**

From [http://www.theregister.co.uk/2015/09/25/us\\_court\\_rules\\_phone\\_passcodes\\_are\\_protected\\_by\\_the\\_fifth\\_amendment/](http://www.theregister.co.uk/2015/09/25/us_court_rules_phone_passcodes_are_protected_by_the_fifth_amendment/)

# Victory - FTC COMMISSIONER SUPPORTS ENCRYPTION

- » High profile car hacks, large-scale breaches of intimate information, news of compromised household appliances -- hardly a day passes without some revelation of the ways in which our increasing interconnectedness is introducing new vulnerabilities into our lives. Technology is advancing at a rapid clip, and so are breaches. Now, more than ever, strong security and end-user controls are critical to protect personal information.
- » Each of us can play an important role in protecting our information on laptops, desktops, and smartphones by using strong end-user controls, such as disk encryption and firmware passwords. Disk encryption can protect information stored on the hard-disk from unwanted access and hardware passwords essentially prevent machines from being used without the password.
- » Using these tools can also make it easier for consumers to recover lost or stolen devices as the FTC's Chief Technologist recently discovered through personal experience.
- » Encryption and end-user protections can raise issues of access for law enforcement. Some argue that data storage and communications systems should be designed with exceptional access -- or "back doors" -- for law enforcement in order to avoid harming legitimate investigative capabilities. However, many technologists contend that exceptional access systems are likely to introduce security flaws and vulnerabilities, weakening the security of products.
- » This debate, sometimes called the crypto wars, is hardly new -- it has been going on in some form or another for decades. But what is changing is the extent to which we are using connected technology in every facet of our daily lives. **If consumers cannot trust the security of their devices, we could end up stymieing innovation and introducing needless risk into our personal security. In this environment, policy makers should carefully weigh the potential impact of any proposals that may weaken privacy and security protections for consumers.**

<http://m.huffpost.com/us/entry/8083756>

**Terrell McSweeney Commissioner, Federal Trade Commission**

# Victory – FTC vs Wyndham: Cybersecurity Under FTC Authority

- » U.S. appellate court granted the Federal Trade Commission (FTC) authority to regulate corporate cybersecurity.
- » Under its new powers, the FTC will continue to “prevent business practices that are anticompetitive, deceptive or unfair to consumers; enhance informed consumer choice and public understanding of the competitive process; and accomplish this without unduly burdening legitimate business activity.” But, the agency now has been given the mantle to protect online security.
- » 2015 FTC won vs Wyndham
- » 2015 – FTC is suing Anthem
- » 2012 - **FTC fines RockYou \$250,000 for storing user data in plain text**
- » 2012 - **FTC tears into Apple, Google over kids' privacy – or lack of**
- » 2011 – **FTV vs RITEAID**
- » Read the **LESSONS LEARNED FROM THE FTC** presentation at <http://www.rajgoel.com/presentations/>

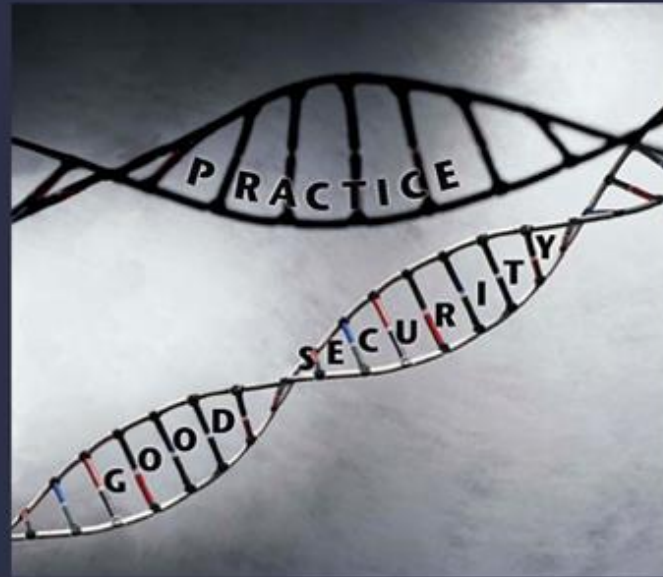
# Victory – Law firms file for class-action status in Target suit

- » Law firms file for class-action status in Target suit
- » Eleven law firms filed with a Minnesota court this past week to ask for class-action certification over Target's 2013 data breach.
- » Eleven law firms filed with a Minnesota court this week to ask for class-action certification over Target's 2013 data breach.
- » The document called Target's payment card security prior to the breach "lackadaisical," and said it directly contributed to its breach. "The evidence already available to date, reveals that both before and during the breach, Target maintained substandard cybersecurity practices, which allowed the inception and caused it to spiral from a controllable event with minimal losses into one of the largest data security breaches in United States history," the motion stated.
- » The law firms represented four banks and a credit union as their lead plaintiffs.
- » Writing that this one case is "vastly superior" to having "thousands of financial institutions" go through the same questions against Target, the lawyers argued in the motion that their clients constitute a class, and the case should continue as a class-action suit.

<http://www.scmagazine.com/minnesota-court-asked-to-consider-class-action-status/article/435503/>

# Smart Cars – unsafe at ANY Speed

- » In July 2015, Chrysler recalled 1.4 million vehicles - researchers were able to control the heating & cooling system, blast the radio, activate the windshield wipers, shut the car down...**from a laptop 10 miles away.**
- » GM **OWNSTAR** gadget allows anyone to locate, unlock, or remote start any **GM, BMW, Mercedes** by intercepting and breaching security of the RemoteLink mobile app.
- » **Progressive Insurance** has placed up to **2 million vehicles** at risk of shutdowns, thefts or mysterious accidents by sending drivers the “**Progressive Snapshot**” dongle.
- » Perhaps it's time to rename **MADD** as “**Mothers Against Dangerous Developers**”.



**NONE OF US ARE BORN WITH A  
“SECURITY GENE”**

 **Defense Security Service (DSS)**  
for Mission, National Security

Security Managers Forum, 2009 Poster Contest  
Industrial Security, 2nd Place Winner



# What to Teach Your Kids, Employees & Interns About Social Media



**“Everything You Say Can And Will Be Used Against You, By Anybody, Now Or Decades Into The Future.” – Falkvinge**

<http://www.brainlink.com/free-stuff/webinars/what-to-teach-your-kids-employees-and-interns-about-social-media/>

# VW caught shipping cheat software

- » Stock dropped more than 20%
- » Proves industry self-regulation doesn't work
- » Who else was gaming tests?
- » Could VW (Chrysler, Tesla, Mercedes Benz, etc) hacks usher in an era of:
  - 3<sup>rd</sup> Party Audited Software?
  - Vendor Software Liability?
  - Put Automanufacturers on the same footing as Aircraft manufacturers?

# Suggestions

1. EDUCATE yourself and the young people in your life on the REALITY of privacy
2. LOBBY your elected officials and others to DEFEND your 1<sup>st</sup>, 4<sup>th</sup> & 5<sup>th</sup> Amendment rights (US) or EU Human Rights
3. Review your foreign travel technology plans
4. JOIN the EFF
5. Adopt the Canadian/PIPEDA Approach
6. Demand a LEMON LAW for Software
7. Keep an eye on the FTC cases

# Final Thoughts

In every generation, a new King John; a new Khrushchev and a new Solzhenitsyn is born. It's OUR job as citizens to DEFEND the rights given to us by our respective constitutions and DEMAND that they be conferred on our WEAKEST citizens, not just the strongest or the wealthiest.

**Privacy is a human right....not a luxury**

# Discuss With Your Kids & Grandparents

## Protect Your Home & Family

**Chapter 1** - Parenting Responsibly In The Internet Era

**Chapter 2** - Has Social Media Gone Unsupervised For Far Too Long?

**Chapter 3** - Grandparents Are Offering Their Grandkids To Predators

**Chapter 4** - Prevent Your Kids From Spending Thousands On In-App Purchases

**Chapter 5** - The Fine Line Between Guidance And Surveillance

## Right To Privacy In The 21st Century

**Chapter 6** - The Right To Digital Privacy

**Chapter 7** - The Paradox Of Not Owning What You Buy

**Chapter 8** - The Myth Of Online Privacy

**Chapter 9** - Information To The Highest Bidder: The Data Exchange Between Government And Private Business

**Chapter 10** - Invasion Of Privacy: Is It The User's Fault?

**Chapter 11** - Ad Blockers Make The Web Safer And Faster!

## The Banes Of Technology

**Chapter 12** - Lessons Learned From Centcom, Crayola And Isis Hackers

**Chapter 13** - The Real Cost Of Facebook

**Chapter 14** - How You Spend Your Time Online Can Be Used Against You

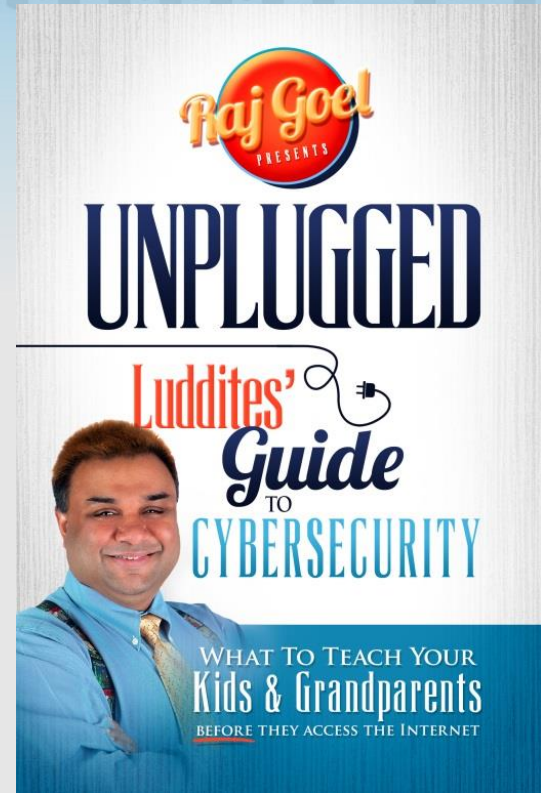
**Chapter 15** - Adult Friend Finder Data Breach – Blackmail R Us?

**Chapter 16** - Welcome To The Age Of Online Dating

**Chapter 17** - Social Security Is Not Secure

**Chapter 18** - Beware The Smart Home Of The Future

**Smart Cars: Unsafe at Any Speed**





The Biggest Threat:

Failing to Pay Attention

Defense Security Service (DSS)  
Our Mission. Your Security.

Security Managers Forum, 2009 Poster Contest  
Insider Threat, 3rd Place Winner

# Contact Information

## Raj Goel, CISSP

Chief Technology Officer  
Brainlink International, Inc.

C: 917-685-7731

raj@brainlink.com

www.RajGoel.com

www.linkedin.com/in/rajgoel

@rajgoel\_ny

Author of

### **UNPLUGGED Luddites Guide To Cybersecurity**

<http://www.amazon.com/UNPLUGGED-Luddites-Guide-CyberSecurity-Grandparents/dp/0984424830/>

### **The Most Important Secrets To Getting Great Results From IT**

<http://www.amazon.com/gp/product/0984424814>

