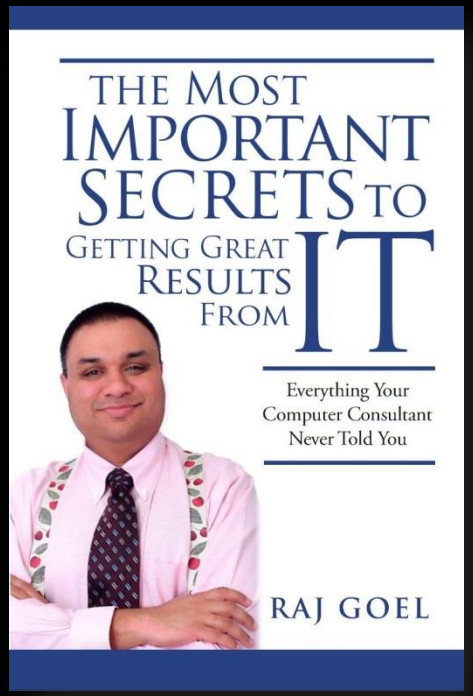
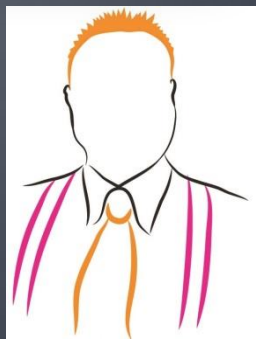
A Global overview of Trends in Private, Corporate and Government Surveillance

Raj Goel, CISSP
Chief Technology Officer
Brainlink International, Inc.
raj@brainlink.com / 917-685-7731





Handouts

Grab them from

www.RajGoel.com/surveillance-notes/

"Privacy OR Security" or "Privacy & Security"

- 1215 – Magna Carta – King John stripped of divine right
- 1628 – Sir Edward Coke establishes "A man's home is his castle" in English common law
- 1791 – US Bill of Rights, 4th Amendment protects citizens from "unreasonable search and seizure"

- Technology has transformed our homes (schools and workplaces) from castles to virtual prisons.

http://www.rajgoel.com/2013/09/privacy-vs-security-what-do-you-choose/

September 21st, 2013

Privacy vs. Security — What do you choose?

Below is an excerpt from the Keynote presentation I delivered at GBATA 2013 in ***Helsinki, Finland.*** *It is based upon my* ***"A Global Overview of Trends in Personal, Corporate and Government Surveillance"*** *presentation. This article also appeared in the* ***Homeland Security Newswire****.*

Those who ask you to choose SECURITY OR PRIVACY and those who VOTE on SECURITY OR PRIVACY are making false choices. That's like asking AIR OR WATER — which do you choose? You need BOTH to live.

Maslow placed SAFETY (of which security is a subset) as 2nd only to food, water, sex and sleep. As humans we CRAVE safety.

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/

Vanity is my favorite sin

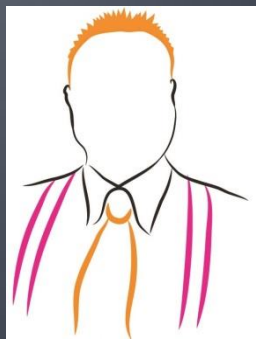
- Al Pacino, The Devils Advocate

"If you have something that you don't want anyone to know maybe you shouldn't be doing it in the first place"

- Eric Schmidt

"The Age Of Privacy is Over"

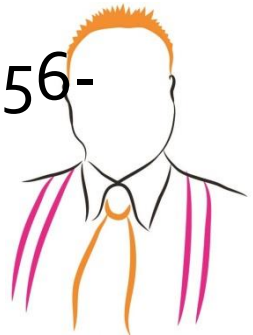
– Mark Zuckerberg



Burglary Ring uses Facebook to choose victims

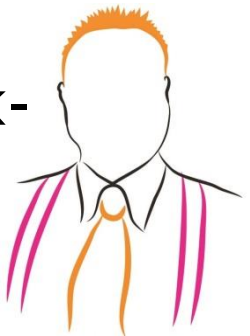
- Burglary Ring in Nashua, NH committed 50 break-ins, stole $100,000+. Targeted victims who posted their location on Facebook.
- http://gawker.com/5635046/real+life-burglary-ring-uses-facebook-to-choose-victims

- Adam Savage, Mythbusters, posted photo of his new truck, parked in front of his house. Fans (and crooks!) discover his address via GeoTags embedded in the photo.
- http://text.broadbandreports.com/forum/r24657556-MythBusters-stalked-down-with-geotag-photos



Say yes to a kegger with a cute girl, pay $227 in fines

- University of Wisconsin-La Crosse student Adam Bauer was ticketed for underage drinking in November 2009 after accepting a friend request from a seemingly good-looking girl on Facebook. The request was actually a ruse from La Crosse police, who had set up a sting to catch underage drinkers. Bauer had posted photos of himself holding a beer, an act that ultimately led to his $227 fine. Bauer was at least one of eight people who said they had been cited for photos posted on social-networking sites.
- http://tech.ca.msn.com/most-notorious-facebook-arrests?page=7



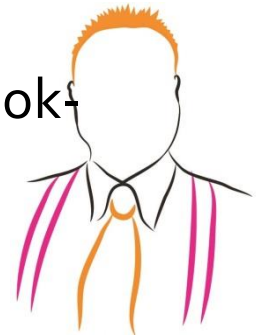
Lose Your Job – 2011 Apple v Crisp (UK)

- Mr. Crisp worked at an Apple Retail store in the UK.
- He posted negative comments about Apple on his Facebook page and marked them PRIVATE.
- First because "Apple had in place a clear social media policy and stressed in their induction process that commentary on Apple products, or critical remarks about the brand were strictly prohibited".
- Despite having "private" Facebook settings, the tribunal decided that there was nothing to prevent friends from copying and passing on Crisp's* comments, so he was unable to rely on the right to privacy contained in Article 8 of the European Convention on Human Rights (covered in the UK by the Human Rights Act 1998). He retained his right to freedom of expression under Article 10, but Apple successfully argued that it was justified and proportionate to limit this right in order to protect its commercial reputation against potentially damaging posts.

http://www.theregister.co.uk/2011/11/03/apple_employee_fired/

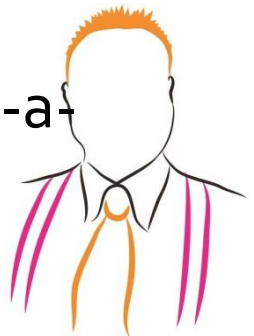
ACMA rules Facebook photos are not private

- Users offered no safety from Facebook-trawling.
- Australia's communications regulator has ruled that television networks are not breaking the industry's code of practice when publishing photos lifted from a public Facebook profile.
- The Australian Communications and Media Authority ACMA determined that Channel Seven did not breach the Commercial Television Industry Code of Practice when it accessed and broadcasted photographs – specifically in the case of a deceased person lifted from a Facebook tribute page, and another which broadcasted the name, photograph and comments penned by a 14-year old boy.
- http://www.itnews.com.au/News/284896,acma-finds-facebook-photos-are-not-private.aspx



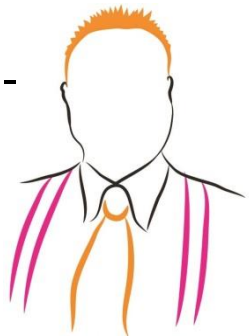
Ehling v. Monmouth-Ocean Hospital Service Corp.

- Non-Public Facebook postings are private and uninvited employers have no right to read them.
- But if your frenemies pass them to your boss…too bad.
  - The court found that the postings were private and protected by the Stored Communications Act, because Ehling had configured her Facebook settings, so only her "friends" could see writings.
  - Ultimately, the court ruled in favor of MONOC based on an exception in the Stored Communications Act, which is part of the federal Electronics Communications Privacy Act. Because Ronco was authorized to see the postings, he could share them with other people, including Ehling's employer.
- http://www.csoonline.com/article/739574/court-ruling-a-warning-to-companies-on-workers-facebook-privacy



Prevent your kids from becoming accidental porn stars

- Children and young people are posting thousands of sexually explicit images of themselves and their peers online, which are then being stolen by porn websites, according to a leading internet safety organisation.
- A study by the Internet Watch Foundation (IWF) reveals that 88% of self-made sexual or suggestive images and videos posted by young people, often on social networking sites, are taken from their original online location and uploaded on to other websites.
- Reams of sexually explicit images and videos are being uploaded by children and young people, the study found. During 47 hours, over a four-week period, a total of 12,224 images and videos were analysed and logged. The majority of these were then mined by "parasite websites" created for the sole purpose of displaying sexually explicit images and videos of young people.
- - http://www.guardian.co.uk/technology/2012/oct/22/parasite-porn-websites-images-videos



Woman arrested for outing cop on Facebook

- A Texas woman (Melissa Walthall) has been arrested and charged with a felony for posting a publicly available photograph of an undercover police officer to her Facebook profile, reports say.According to the Associated Press, Melissa Walthall, 30, of Mesquite, Tex., was arrested last week and charged with retaliation, a felony, for posting the photo.

- - http://www.huffingtonpost.com/2012/10/16/melissa-walthall-texas-undercover-cop-facebook-arrest_n_1970479.html?utm_hp_ref=technology

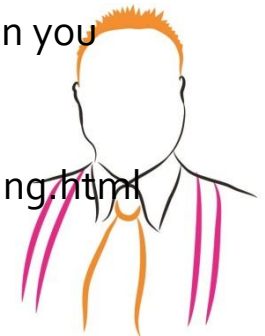
Facebook can hurt your Credit Rating

- You know those deadbeat friends of yours on Facebook? They could end up killing your credit score and costing you a loan. At the very least, your no-account pals could bump up your interest rate.
- […] details the efforts of several online banks that plan to analyze your social media profiles to determine how big a credit risk you are. It's yet more evidence that, unlike Las Vegas, what happens on Facebook doesn't stay on Facebook – and could come back to bite you in unexpected and unpleasant ways.

- How are banks going to use this information? First, they're going to use your friends list to troll for future prospects. If you just took out a line of credit against the equity in your house, maybe your friends will too – assuming they've got any equity left.

- It gets worse. Let's say you fall a few months behind on your payments and you've decided to banish the bill collecting goons to voice mail. Hong Kong-based micro-lender Lenddo – which asks for your Facebook, Twitter, Gmail, Yahoo, and Windows Live logons when you sign up — reserves the right to rat you out to all your friends

- http://www.pcworld.com/article/246511/how_facebook_can_hurt_your_credit_rating.html



The UN-social Network

Facebook a top cause of relationship trouble, say US lawyers

Social networking site becoming primary source of evidence in divorce proceedings and custody battles, lawyers say

Richard Adams in Washington
guardian.co.uk, Tuesday 8 March 2011 14.26 EST
Article history

Photographs taken from social networking sites are a rich source of evidence, divorce lawyers say. Photograph: Chris Jackson/Getty Images

When Facebook gets involved, relationships can quickly fall apart – as Hosni Mubarak and Muammar Gaddafi have discovered. But dictatorships are not the only ties being dissolved by social networking sites: now Facebook is increasingly being blamed for undermining American marriages.

Even though the rate of divorce in the US has remained largely stable in recent years, American divorce lawyers and academics have joined Middle East analysts in picking out Facebook as a leading cause of relationship trouble, with American lawyers now demanding to see their clients' Facebook pages as a matter of course before the start of proceedings.

http://www.guardian.co.uk/technology/2011/mar/08/facebook-us-divorces

The Facebook divorces: Social network site is cited in 'a THIRD of splits'

By JOHN STEVENS

Last updated at 9:07 PM on 30th December 2011

Comments (71) | Share | +1 7 | Tweet 229 | Like 831

Facebook is becoming a major factor in marriage breakdowns and is increasingly being used as a source of evidence in divorce cases, according to lawyers.

The social networking site was cited as a reason for a third of divorces last year in which unreasonable behaviour was a factor, according to law firm Divorce-Online.

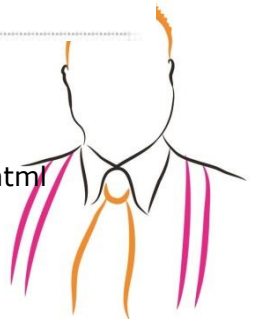
The firm said it had seen a 50 per cent jump in the number of behaviour-based divorce petitions that contained the word 'Facebook' in the past two years.

Nasty surprise: A third of the 5,000 petitions filed with Divorce-Online in the past year mentioned Facebook

Mark Keenan, managing director of Divorce-Online, said: 'Facebook has become the primary method for communicating with friends for many people.

'People contact ex-partners and the messages start as innocent, but lead to trouble.

http://www.dailymail.co.uk/femail/article-2080398/Facebook-cited-THIRD-divorces.html



WOW & Farmville logs used in Divorces

- According to the American Academy of Matrimonial Lawyers, 81% have used or faced evidence from Facebook, MySpace, WOW, Twitter, LinkedIn, etc. See http://kotaku.com/5576262/farmville-world-of-warcraft-are-divorce-lawyers-latest-weapons-in-court and http://www.usatoday.com/tech/news/2010-06-29-facebook-divorce_N.htm?loc=interstitialskip

- For example
  - 1. Father seeks custody of the kids, claiming (among other things) that his ex-wife never attends the events of their young ones. Subpoenaed evidence from the gaming site World of Warcraft tracks her there with her boyfriend at the precise time she was supposed to be out with the children.
  - 2. Mom denies in court that she smokes marijuana but posts partying, pot-smoking photos of herself on Facebook.

Facebook video leads to arrest of two teens

- Madison police say two young teens have been arrested after video of their street fight was posted to Facebook.
- A Capital Times report on Tuesday says the video showed adults standing around watching the boys fight in the street last week. No serious injuries were reported.
- Police say the fight lasted about 2½ minutes. The video shows a 14-year-old repeatedly slamming the head of a 13-year-old into the pavement. The younger boy told police he may have blacked out briefly.
- Police began to investigate after they learned of a video of the fight that one of the boys had posted on his Facebook page.
- The teens were arrested on tentative charges of battery and disorderly conduct.
- http://www.fox11online.com/dpp/news/wisconsin/facebook-video-leads-to-arrest-of-two-teens

Facebook outs most personal secrets

- Bobbi Duncan desperately wanted her father not to know she is lesbian. Facebook told him anyway.
- One evening last fall, the president of the Queer Chorus, a choir group she had recently joined, inadvertently exposed Ms. Duncan's sexuality to her nearly 200 Facebook friends, including her father, by adding her to a Facebook Inc. discussion group. That night, Ms. Duncan's father left vitriolic messages on her phone, demanding she renounce same-sex relationships, she says, and threatening to sever family ties. The 22-year-old cried all night on a friend's couch. "I felt like someone had hit me in the stomach …

- http://online.wsj.com/article/SB10000872396390444165804578008740578200224.html

Facebook likes considered key evidence in terrorist plot

- That doesn't mean that there still aren't some oddities in the case, however. As a number of folks have sent over, reading through the indictment (also embedded below) shows that a significant chunk of the "evidence" seems to consist of Facebook "likes" and shared content among the accused. From the indictment:
- I have reviewed several of the social media web sites for KABIR, SANTANA, DELEON, each of whom has posted radical prom jihad content on their respective pages. Additionally, portions of the social media show that DELEON and SANTANA "liked" postings on KABIR's Facebook page as early as May 2011.
- Public items posted by KABIR to his social media accounts include photographs of himself, non-extremist content, radical Islamist content, and items reflecting a mistrust of mainstream media, abuses by the government, conspiracy theories, abuses by law enforcement, and the war in Afghanistan. …

http://www.techdirt.com/

Vice Magazine failed to strip photo metadata – McAfee arrested

- John McAfee, the millionaire software executive turned semi-fugitive, was falsely reported captured over the weekend. Now, in a new post on his blog, he claims that he's left Belize for another country in the company of two Vice journalists and his longtime female companion, Sam. He also noted that Vice would be publishing a story today that would end all the speculation as to whether or not he is a "drug-crazed madman."can be charged with cyber-libel," the senator said.
- http://www.wired.com/gadgetlab/2012/12/oops-did-vice-just-give-away-john-mcafees-location-with-this-photo//

Michael Dell's kids' tweet undermines $2.7M security efforts

- Dell spends $2.7 million per year to protect founder Michael Dell's family, but tweets and blogs from the billionaire's kids describing where they are and what they're doing don't make the job any easier.
- An Instagram account linked to the Twitter postings of Dell's daughter, Alexa, 18, divulged where she was shopping and where she stayed on a recent trip to New York. Alongside that, her tweets detailed GPS information that could track her exact location; she even tweeted the location of her high school graduation dinner, which her family attended.
- A photo of Zachary Dell, 15, appeared on a Tumblr blog called "Rich Kids of Instagram," showing the scion devouring a grand buffet just before departing for Fiji on the family's jet.

http://www.foxnews.com/tech/2012/08/13/dell-faces-major-security-breach-over-daughter-tweets

Zuckerberg's sister caught in Facebook Photo brouhaha

- Mark's sister posted a family photo.
- Photo showed up on someone else's newsfeed, friend tweeted it.
- Randi Zuckerberg said that the sharing of a private photo was 'not about privacy settings, it's about human decency'.

- "Not sure where you got this photo," Zuckerberg wrote, in subsequently deleted correspondence captured by BuzzFeed. "I posted it only to friends on FB. You reposting it on Twitter is way uncool."

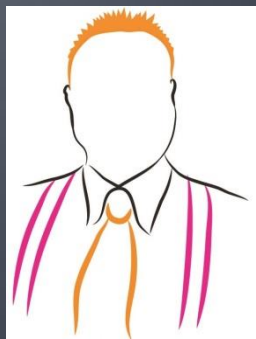
http://www.guardian.co.uk/technology/us-news-blog/2012/dec/27/facebook-founder-sister-zuckerberg-photo

TECHNO HUBRIS

We know where you are. We know where you've been. We can more or less know what you're thinking about."

"Streetview the cars we drive only once, you can just move, right?"

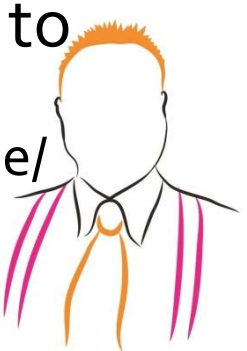
"I ACTUALLY think most people don't want Google to answer their questions, they want Google to tell them what they should be doing next.



Automatic Facebook couple pages – uncomfortable data mining

- Facebook users who have listed themselves as "In a Relationship" or "Married" and linked their profile to their partner's will find that Facebook has automatically generated them a couple page, celebrating their love. The couple's page skims off a photo of the happy pair together as the profile picture, lists all events that the two have mutually attended and the Likes that they have in common. It shows all photos that both are tagged in and lists wall posts that each have put on the other's wall.
- You don't need to be a dyspeptic technology hack to find this nauseating.

http://www.theregister.co.uk/2012/11/15/facebook_couples_page/



Find ANYONE on Facebook – just guess their phone number

- On Friday, a researcher by the name of Suriya Prakash claimed that the majority of phone numbers on Facebook are not safe. It's not clear where he got his numbers from (he says 98 percent, while another time he says 500 million out of Facebook's 600 million mobile users), but his demonstration certainly showed he could collect countless phone numbers and their corresponding Facebook names with very little effort.
- Facebook has confirmed that it limited the Prakash's activity but it's unclear how long it took to do so. Prakash disagrees with when Facebook says his activity was curtailed.

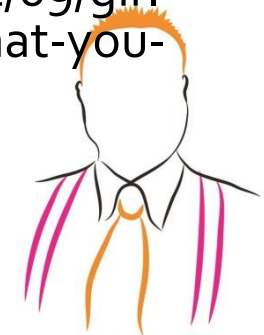
- This is not a bug, but a FEATURE of facebook.

http://thenextweb.com/facebook/2012/10/10/facebook-confirms-researcher-exploited-privacy-settings-to-quickly-collect-user-phone-numbers//

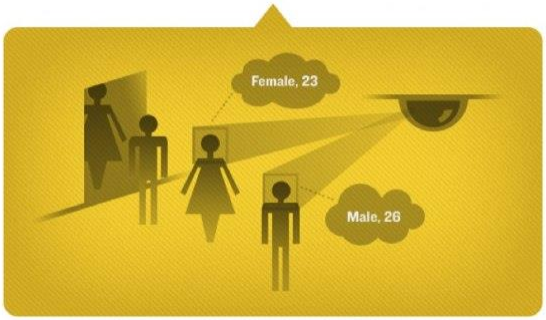
Girls Around Me

- As far as I can tell, the app "Girls Around Me" wasn't violating any laws. But it was high on the creepy scale when, according to reports, women's identity, photographs and location were being revealed to strangers, even though the women never opted into the service. Although the developer, Moscow-based I-Free, hardly deserves any awards, the app's a good wake-up call for people to use the privacy settings of legitimate social networking and location services.
- The app mashed together information people posted about themselves publicly on Foursquare and Facebook and created a map showing the location and photographs of nearby women.

http://www.forbes.com/sites/larrymagid/2012/04/09/girls-around-me-app-is-a-reminder-to-be-aware-what-you-share/



SceneTap

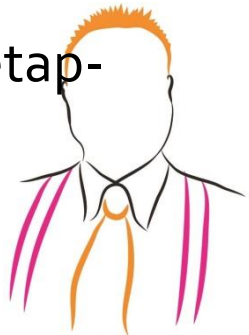


- Remember all those movies where the hero ducked into a bar to avoid the bad guys?
- Or all those bars you walked into with your date, because the vibe felt right?

- Kiss those days good bye.

- Bars equipped with SceneTap record all patrons in real time, perform gender & demographic analysis, and publish that data on the web & mobile apps.
- So much for the privacy and anonymity of your local bar…

- http://venturebeat.com/2012/05/13/scenetap-is-watching/



India is building the largest Biometrics database in the world

- 1.2 Billion users
- All 10 fingers & both irises
- 300 million people already enrolled.
- 400 million by end of 2014

- State agencies and other entities allowed to ask questions above the Federal limit – Caste, Religion, etc.
- API allows access by Law Enforcement, Banks, Corporations, Other entities

- At completion, 20PB of data – 128x bigger than DHS' database

- 99% effective.
- 1% error rate = 12 million faulty records per day

http://www.wired.com/magazine/2011/08/ff_indiaid/all/

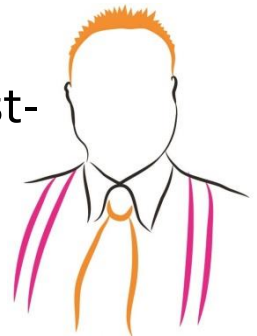
UAE holds world record for largest Biometric database

- 103 million fingerprints
- 15 million faces
- Digital Signatures

- 14 Million records in Sep 2009, 102 million by Sep 2012

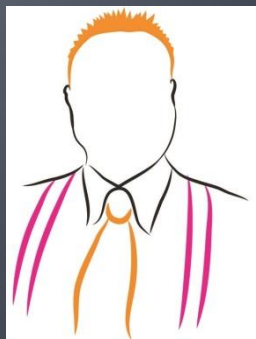
- They sought World Record Academy recognition for having the largest biometric database in the world in Oct 2012

http://gulfnews.com/news/gulf/uae/government/uae-has-largest-biometric-database-1.1117910



For my friends, anything. For my enemies, the law.

- Oscar Benavides, former Peruvian President

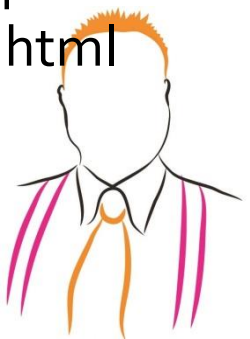


ECPA - Electronic Communications Privacy Act (1986)

- ECPA declared that e-mail was a private means of communication, and that we might hope for the same level of privacy in it as we have in phone calls and letters. Among other things, it means that police need a wiretap warrant to read your e-mails, and that your e-mail company's employees can't disclose your e-mails to others.
- [...] E-mail in transit is protected, but those in law enforcement advocate that once mail is processed and stored, it is no longer the same private letter, but simply a database service.

- GMail's big selling point is that they don't simply deliver your mail. They store it for you, and they index it so you can search it.

- - Brad Templeton, Chairman of the Electronic Frontier Foundation, http://www.templetons.com/brad/gmail.html



What can we learn about ECPA and Patriot Act from the Petraeus affair?

- If former CIA Director David Petraeus had secretly stashed love letters he exchanged with his paramour at home under his mattress, he might have actually done a better job of protecting his privacy.
- Because of the way a key federal privacy law was worded in 1986, back in the pre-Internet days of analog modems, floppy disks, and the 2.8 MHz Apple IIgs, e-mail stored in the cloud receives less legal protection than it would if printed out.
- For love letters stashed under a mattress, FBI agents would have had to secure a search warrant from a judge to enter Petraeus' bedroom. Perhaps just as important, he would likely have known that his house had been raided. Front doors bashed in with a "Hydra Ram" forcible entry tool tend to make that obvious. So does Rule 41 of the Federal Rules of Criminal Procedure.
- But for love letters stored in draft format on Gmail, something that Petraeus and biographer Paula Broadwell reportedly did, the Justice Department claims that police have the right to access those without a search warrant. It says only a subpoena, signed by a prosecutor without a judge's prior approval and without demonstrating probable cause related to a crime, is necessary.

http://news.cnet.com/8301-13578_3-57550072-38/petraeus-e-mail-affair-highlights-u.s-privacy-law-loopholes/

PATRIOT Act – Global Reach

Moving Data from Country to Country: European Safe Harbor

One issue is that data can flow from country to country, especially from the US to Europe, in which case assurances about the security of the data must follow the Safe Harbor protocols.

The EU prohibits personal data from crossing borders into other countries except under circumstances in which the transfer has been legitimated by a recognized mechanism, such as the "Safe Harbor" certification

To allow for the continual flow of information required by international business, the European Commission and the U.S. Department of Commerce reached agreement, whereby U.S. organizations can self-certify as complying with the Safe Harbor principles. Microsoft Online Services can transfer data from the EU to the U.S. for processing because Microsoft is Safe Harbo certified. Microsoft was first certified under the Safe Harbor program in 2001, and the LCA Regulatory Affairs team recertifies compliance with the Safe Harbor Principles every twelve months

All of this implies that data security has been transformed from a local entity to a country wide operation. Should the US or European governments suspect that data is being used by terrorists or potential terrorists, it will be subject to investigation.

http://www.windows7news.com/2011/06/23/patriot-act-azure-cloud-security/

Irish Govt warns against using MS, Amazon, Google, etc.

2010
02.07

Irish Government Warns Against Using Microsoft Azure And Others

Category: Commentary / Tags: no tag / Add Comment

Yesterday the Irish Times (no links from me to them because they hosted outside of Ireland after consultin a number of companies here in 2007) had an article that featured a government internal email from the Irish Department of Finance. It instructed the various departments and organisations within the government to be wary of using cloud services and it specifically mentioned Microsoft as an example. The reasons included security and Data Protection Act compliance.

The problem is the USA Patriot Act. Any American owned hosting service or data centre, no matter what country it is in, must comply with the Patriot Act. That gives the USA federal government the right to demand instant access to any data hosted by that service. It doesn't matter if Amazon has a data centre in Ireland or if Microsoft has a data centre in Ireland or the Netherlands. They're both American, they both must comply with the Patriot Act, and therefore any organisation storing sensitive or personal information should not be using those services, or services hosted on those platforms for storing that data.

http://www.aidanfinn.com/?p=10367

Patriot Act can "obtain" data in Europe, researchers say

- European data stored in the "cloud" could be acquired and inspected by U.S. law enforcement and intelligence agencies, despite Europe's strong data protection laws, university researchers have suggested.
- The research paper, titled "Cloud Computing in Higher Education and Research Institutions and the USA Patriot Act," written by legal experts at the University of Amsterdam's Institute for Information Law, support previous reports that the anti-terror Patriot Act could be theoretically used by U.S. law enforcement to bypass strict European privacy laws to acquire citizen data within the European Union.
- The Patriot Act, signed into law in 2001, granted some new powers to U.S. authorities, but it was mainly a "framework law" that amended and strengthened a variety of older laws, such as the Foreign Intelligence Services Act (FISA) and the Electronic Communications Privacy Act (ECPA).
- "Most cloud providers, and certainly the market leaders, fall within the U.S. jurisdiction either because they are U.S. companies or conduct systematic business in the U.S.," Axel Arnbak, one of the authors of the research paper, told CBS News.

http://www.cbsnews.com/8301-205_162-57556674/patriot-act-can-obtain-data-in-europe-researchers-say/

Thomas Drake, NSA Whistleblower

- Trailblazer was commissioned from the Science Applications International Corporation at a cost of $280 million and never worked as intended, while violating the laws on privacy. The final bill for the project, which was cancelled in 2003, is estimated to be over a billion dollars.
- But Drake warned that the NSA has not learned its lesson from the incident, and that it was one of the NSA's deepest, darkest secrets that it had effectively turned online America into a foreign country for legal purposes. More worrying, similar lax attitudes are now pervasive in the corporate world.
- "Industry self-regulation is not working, contrary to what you have seen or heard," he warned. "Let's not kid ourselves. It's also patently disingenuous to say that no names are collected, only a computer number, when the technology is out there to discover everything about you electronically."

- http://www.theregister.co.uk/2011/10/19/nsa_whistleblower_intelligence_thinthread/

Senator Ron Wyden (D) Oregon

- Wyden was also scathing about the **Patriot Act, pointing out that there were in fact two forms of the legislation, the public law and the interpretation of it by government -** the latter being secret. He said that if the American people could see what the secret interpretation was they would be surprised and angry. He said he would love to lay out the way the act was being used, but was bound by secrecy rules.

http://www.theregister.co.uk/2011/10/18/riaa_biggest_threat_innovation_senator/

Saudi Arabia implements electronic surveillance on women

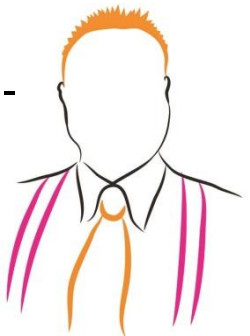
- Denied the right to travel without consent from their male guardians and banned from driving, women in Saudi Arabia are now monitored by an electronic system that tracks any cross-border movements.
- Since last week, Saudi women's male guardians began receiving text messages on their phones informing them when women under their custody leave the country, even if they are travelling together.
- Manal al-Sherif, who became the symbol of a campaign launched last year urging Saudi women to defy a driving ban, began spreading the information on Twitter, after she was alerted by a couple.

  http://www.rajgoel.com/saudi-arabia-implements-electronic-surveillance-on-women

New York City Police Amassing a Trove of Cellphone Logs

- When a cellphone is reported stolen in New York, the Police Department routinely subpoenas the phone's call records, from the day of the theft onward. The logic is simple: If a thief uses the phone, a list of incoming and outgoing calls could lead to the suspect.
- But in the process, the Police Department has quietly amassed a trove of telephone logs, all obtained without a court order, that could conceivably be used for any investigative purpose.The call records from the stolen cellphones are integrated into a database known as the Enterprise Case Management System, according to Police Department documents from the detective bureau.

  http://www.nytimes.com/2012/11/27/nyregion/new-york-city-police-amassing-a-trove-of-cellphone-logs.html



RIM hands over BBM messages to London Police

RIM to turn in BlackBerry-using looters after London riots

Empathetic RIM plans to help police

By **Paul Kunert** · **Get more from this author**

Posted in Policing, 8th August 2011 15:42 GMT

BlackBerry UK has broken silence over the role its devices played in helping disaffected London yoof co-ordinate riots in Tottenham, Brixton, Enfield and Walthamstow this weekend

The smash 'n' burn attacks on High Street stores and vehicles on Saturday and yesterday came days after the death of Mark Duggan, who was killed in an alleged shoot out with police.

But unlike the Arab spring protests, which used the very public social media forums Facebook and Twitter to rally the troops, BlackBerry's version of IM was the favoured mode in the capital according to anecdotal evidence.

BlackBerry UK – the official Twitter account for the troubled smartphone maker RIM – made a move away from dishing out technical advice to users.

"We feel for those impacted by the riots in London. We have engaged with the authorities t assist in any way we can," it stated

http://www.theregister.co.uk/2011/08/08/blackberry_riots/

RIM creates backdoor for Indian Police

RIM backdoor access for Indian probers

Mumbai centre up and running since earlier this year

By **Anna Leach** • **Get more from this author**

Posted in Wireless, 28th October 2011 17:01 GMT

RIM has opened a monitoring centre in Mumbai to help the Indian government sip data fi Blackberry users there, said the *Wall Street Journal* today, quoting unnamed sources.

The Canadian firm opened the small facility earlier this year to deal with requests from ndian intelligence agencies, the paper reports. RIM will hand over messages and emails from suspect individuals to the Indian government – providing it is satisfied that the demands are legally justified.

t is encrypted email and BBM messages in particular that Indian cops are interested in, t ndian government reportedly fearing that the messaging channels could be used for organising terrorist attacks. RIM can't hand over corporate emails, because individual companies hold the keys to that information. However India seems to be satisfied with the current compromise that gives it access to consumer accounts.

The *Wall Street Journal* said RIM was no longer facing the prospect of shutdowns by the

http://www.theregister.co.uk/2011/10/28/blackberry_help_indian_government_sip_data/

Facebook bug leaks contact info of 6 million users

- In an advisory posted on Friday, Facebook's security team explained that the code the social network uses to make friend recommendations inadvertently caused the email addresses and phone numbers of potential contacts to be associated with other users' account data.
- If those users then used the DYI tool, the wrongly added contact information would be included in the download, whether or not the users were actually friends with the owners of the addresses or numbers in question.

http://www.theregister.co.uk/2013/06/21/facebook_contact_leak/

WIRED – Carriers fulfilled 1.3MM cell phone surveillance in 2011

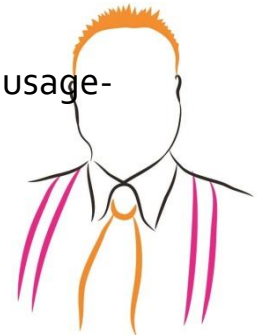
- Mobile carriers responded to a staggering 1.3 million law enforcement requests last year for subscriber information, including text messages and phone location data, according to data provided to Congress.
- Nine mobile phone companies forwarded the data as part of a Congressional privacy probe brought by Rep. Edward Markey, (D-Massachusetts), who co-chairs the Congressional Bi-partisan Privacy Caucus.
- The number of Americans affected each year by the growing use of mobile phone data by law enforcement could reach into the tens of millions, as a single request could ensnare dozens or even hundreds of people. Law enforcement has been asking for so-called "cell tower dumps" in which carriers disclose all phone numbers that connected to a given tower during a certain period of time.
- So, for instance, if police wanted to try to find a person who broke a store window at an Occupy protest, it could get the phone numbers and identifying data of all protestors with mobile phones in the vicinity at the time — and use that data for other purposes.

  - http://www.wired.com/threatlevel/2012/07/massive-phone-surveillance/

Australian Police spy on email, web usage without warrants

- Scott Ludlam, Greens senator … "We've already taken some pretty dangerous steps … towards the surveillance state."
- LAW enforcement and government departments are accessing vast quantities of phone and internet usage data without warrants, prompting warnings from the Greens of a growing "surveillance state" and calls by privacy groups for tighter controls.
- Figures released by the federal Attorney-General's Department show that federal and state government agencies accessed telecommunications data and internet logs more than 250,000 times during criminal and revenue investigations in 2010-11.
- The Greens senator Scott Ludlam highlighted the statistics while calling for tighter controls on access to mobile device location information

http://www.theage.com.au/technology/technology-news/police-spy-on-web-phone-usage-with-no-warrants-20120217-1tegl.html



DOJ: We don't need warrants for e-mail, Facebook chats

- An FBI investigation manual updated last year, obtained by the ACLU, says it's possible to warrantlessly obtain Americans' e-mail "without running afoul" of the Fourth Amendment.
- The U.S. Department of Justice and the FBI believe they don't need a search warrant to review Americans' e-mails, Facebook chats, Twitter direct messages, and other private files, internal documents reveal.
- Government documents obtained by the American Civil Liberties Union and provided to CNET show a split over electronic privacy rights within the Obama administration, with Justice Department prosecutors and investigators privately insisting they're not legally required to obtain search warrants for e-mail. The IRS, on the other hand, publicly said last month that it would abandon a controversial policy that claimed it could get warrantless access to e-mail correspondence.

  - May 8, 2013 – CNET - http://news.cnet.com/8301-13578_3-57583395-38/doj-we-dont-need-warrants-for-e-mail-facebook-chats/

6 Seconds of Real-time interception has more privacy than 6 years of Email

- If attorney general Eric Holder wanted to perform even a momentary Internet wiretap on Fox News' e-mail accounts, he would have had to persuade a judge to approve what lawyers call a "super search warrant."
- A super search warrant's requirements are exacting: Intercepted communications must be secured and placed under seal. Real-time interception must be done only as a last resort. Only certain crimes qualify for this technique, the target must be notified, and additional restrictions apply to state and local police conducting real-time intercepts.
- DOJ was able to obtain a normal search warrant -- lacking those extensive privacy protections -- that allowed federal agents to secretly obtain up to six years of email correspondence between Fox News correspondent James Rosen and his alleged sources.

  - May 25, 2013 – CNET - http://news.cnet.com/8301-13578_3-57586211-38/why-doj-didnt-need-a-super-search-warrant-to-snoop-on-fox-news-e-mail/

Justice Department tries to force Google to hand over user data

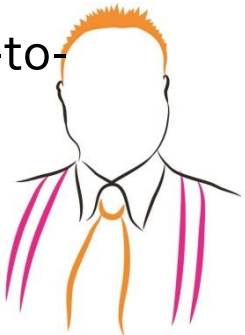
- Secret lawsuit in Manhattan filed last month asks judge to force Google to cough up user data without a search warrant. A different court has already ruled that the process is unconstitutional.
- An inspector general's report (PDF) found that the FBI made 50,000 NSL requests in 2006, and 97 percent of those included mandatory gag orders. NSLs can demand user profile information, but the law does not permit them to be used to obtain the text of e-mail messages or most log files. (Even if NSLs are eventually ruled unconstitutional, the FBI would still have a formidable array of investigative tools including subpoenas, court orders, search warrants, wiretap orders, pen registers, sneak and peek warrants, and surveillance under the Foreign Intelligence Surveillance Act.)

  - May 31, 2013 – CNET - http://news.cnet.com/8301-13578_3-57587005-38/justice-department-tries-to-force-google-to-hand-over-user-data/

Secret warrant used to access WikiLeaks volunteer's Gmail account

- Newly revealed court documents from the Justice department's investigation of WikiLeaks show that the government issued a secret search warrant to Google in order to access all of the email belonging to Herbert Snorrason. He had "helped managed WikiLeaks' secure chat room in 2010," *Wired* reports, and presumably that association is the reason the government demanded his records from Google.

  http://www.theverge.com/2013/6/22/4453722/secret-warrant-used-to-access-wikileaks-volunteers-gmail-account



German Government distributes Trojan

- Five German states have admitted using a controversial backdoor Trojan to spy on criminal suspects.
- Samples of the so-called R2D2 (AKA "ozapftis") Trojan came into the possession of the Chaos Computer Club (CCC), which published an analysis of the code last weekend.
- German federal law allows the use of malware to eavesdrop on Skype conversations. But the CCC analysis suggests that the specific Trojan it wrote about is capable of a far wider range of functions than this – including establishing a backdoor on compromised machines and keystroke logging.

http://www.theregister.co.uk/2011/10/12/bundestrojaner/

GCHQ taps fibre-optic cables for secret access to world's communications

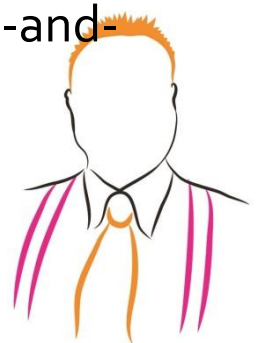
- British spy agency collects and stores vast quantities of global email messages, Facebook posts, internet histories and calls, and shares them with NSA

  http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa?CMP=twt_gu

Law firms, telecoms giants and insurance companies routinely hire criminals to steal rivals' information

- The Serious Organised Crime Agency (Soca) knew six years ago that law firms, telecoms giants and insurance were hiring private investigators to break the law and further their commercial interests, the report reveals, yet the agency did next to nothing to disrupt the unlawful trade.

http://www.independent.co.uk/news/uk/crime/the-other-hacking-scandal-suppressed-report-reveals-that-law-firms-telecoms-giants-and-insurance-companies-routinely-hire-criminals-to-steal-rivals-information-8669148.html



Lithuania uses Google Street view to catch Tax Evaders

- Streetview captured a woman climbing into her hammock in the front yard her. The photograph is now being used as evidence in a tax-evasion case brought by Lithuanian authorities against the undisclosed owners of the home.
- Tax authorities have spent months combing through footage looking for unreported taxable wealth.
- "We were very impressed," said Modestas Kaseliauskas, head of the State Tax Authority. "We realized that we could do more with less and in shorter time."
- More than 100 people have been identified so far after investigators compared Street View images of about 500 properties with state property registries looking for undeclared construction.

  - Wall Street Journal, http://online.wsj.com/article/SB10001424127887324125504578511182111677320.html

PRISM – How & What

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

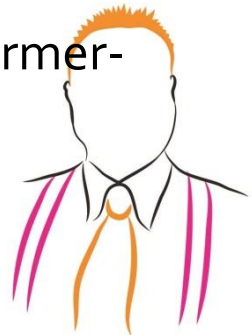
PRISM – The Players

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

Facebook's Former Security Chief Now Works for the NSA

- About a year after Facebook reportedly joined PRISM, Max Kelly, the social network's chief security officer left for a job at the National Security Agency
- The Chief Security Officer at a tech company is primarily concerned with keeping its information inside the company.
- Now working for an agency that tries to gather as much information as it can, Kelly's new job is sort of a complete reversal.

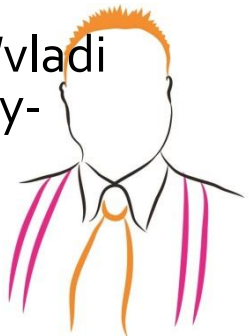
http://www.theatlanticwire.com/technology/2013/06/facebooks-former-security-chief-now-works-nsa/66432/



Vladimir Putin defends the U.S. on spying programs, drones and Occupy Wall Street

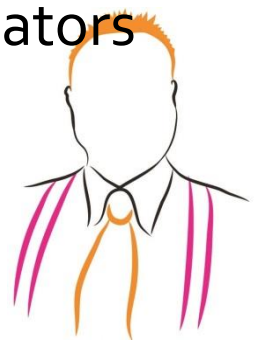
- Russian President Vladimir Putin called the massive U.S. surveillance programs, revealed last week by former NSA contractor Edward Snowden, "generally practicable" and "the way a civilized society should go about fighting terrorism." His comments, made in a far-ranging interview to the state-backed news network RT, seemed to defend programs that have been deeply controversial in the United States and much of Europe, offering an endorsement that the Obama administration is probably not thrilled to receive.
- He said of the New York city police response to Occupy Wall Street, in a comment that seemed consistent with much of his sympathy toward controversial U.S. programs, "**That's the way it's done in the U.S., and that's the way it's done in Russia."**

http://www.washingtonpost.com/blogs/worldviews/wp/2013/06/13/vladimir-putin-defends-the-u-s-on-spying-programs-drones-and-occupy-wall-street/



The best way to predict the future is to invent it. - Alan Kay, Xerox Parc

- Want a blueprint on how to control the internet? Learn from China
- All important foreign sites are cloned for the Chinese audience
- Servers MUST be located in China
- Companies are required to self-censor AND pay for censors
- 50-cent Army publishes government narrative
- Regions can be isolated from the internet without users being aware
  - Developed by Cisco, Blue Coat Systems (friend to dictators everywhere)
  - Refined by China

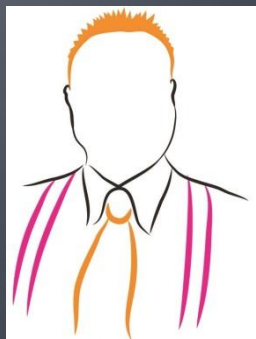


Who did China learn from?

- Stuxnet was a targetted cyber-weapon
- US hacked
  - Chinese mobiles phones
  - Grabbed Chinese SMS data
  - Hacked PacTel telecom
  - Hacked Tsinghua University network repeatedly

The Future is already here. It's just not very evenly distributed.

- William Gibson, Author, futurist



Social Security Numbers – A Brief History

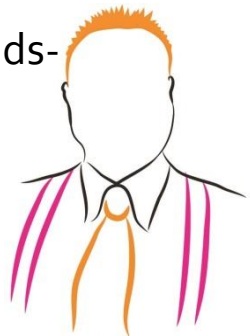
- 1936 - SSNs established
- 1938 - Wallet manufacturer includes secretary's SSN card inside a wallet. 40,000 people thought it was their SSN. 12 people used it in 1977.
- Pre-1986 - kids under 14yrs not required
- Post-1990 - Kids get SSN # with Birth Certificate
- Repeatedly, laws state that "we" oppose the creation of a national ID card. SSNs become defacto national ID numbers.
- Result: Experian, TransUnion, Equifax

http://en.wikipedia.org/wiki/Social_Security_number
http://www.socialsecurity.gov/history/ssn/ssnchron.html

Social Security Numbers Fraud – Target: Kids

- The numbers are run through public databases to determine whether anyone is using them to obtain credit. If not, they are offered for sale for a few hundred to several thousand dollars.
- Because the numbers often come from young children who have no money of their own, they carry no spending history and offer a chance to open a new, unblemished line of credit. People who buy the numbers can then quickly build their credit rating in a process called "piggybacking," which involves linking to someone else's credit file.
- If they default on their payments, and the credit is withdrawn, the same people can simply buy another number and start the process again, causing a steep spiral of debt that could conceivably go on for years before creditors discover the fraud.

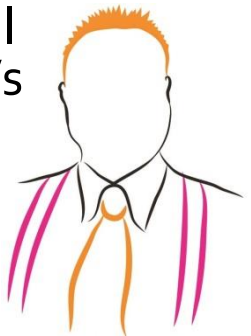
  http://www.foxnews.com/us/2010/08/02/ap-impact-new-id-theft-targets-kids-social-security- numbers-threaten-credit-737395719/



IBM bans Dropbox, Siri, iCloud

- IBM has banned employees from using Dropbox and Apple's iCloud at work as it claws back permission to use third-party cloud services. The rethink has also resulted in a edict against the iPhone 4S's Siri voice recognition technology at Big Blue.
- Jeanette Horan, IBM's chief information officer, told MIT's Technology Review that the restrictions had been applied following a review of IBM's Bring Your Own Device BYOD Policy, introduced in 2010. IBM still supplies BlackBerrys to about 40,000 of its 400,000 employees, but a further 80,000 others now access its intranet using rival smartphones and tablets, including kit they purchased themselves. The [BYOD - ed.] initiative has not yielded anticipated cost reductions even though it has created various security headaches.
- An internal survey of IBM workers discovered they were "blissfully unaware" about the security risks from popular apps, according to Horan. In some cases, staff forwarded internal corporate emails to webmail inboxes, potentially pushing sensitive information beyond Big Blue's security perimeter.

  - http://www.theregister.co.uk/2012/05/25/ibm_bans_dropbox_siri/



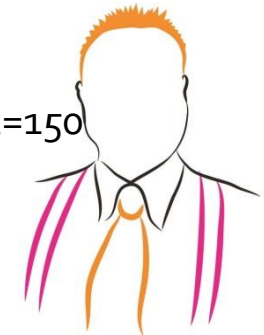
Sites to Bookmark

- www.PleaseRobMe.com
- www.WeKnowWhatYoureDoing.com
- http://www.economist.com/news/special-report/21574628-internet-was-expected-help-democratise-china-instead-it-has-enabled
- http://www.rajgoel.com/tag/social-media-risks/

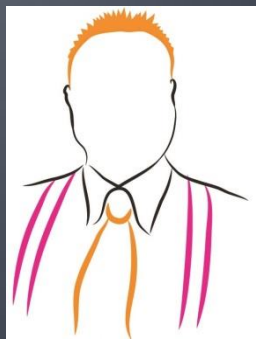
Wozniak on PRISM, Cloud, Russia

- In communist Russia 'you couldn't own anything, and now in the digital world you hardly own anything anymore (YouTube video). You've got subscritpions and you already said ok, ok, agree and you agree that every right in the world belongs to them and you got no rights and anything you put in the cloud, you don't even know,' says Woz. 'Ownership was what made America different than Russia.'"

http://www.youtube.com/watch?feature=player_embedded&v=xOWDwKLJAfo#at=150



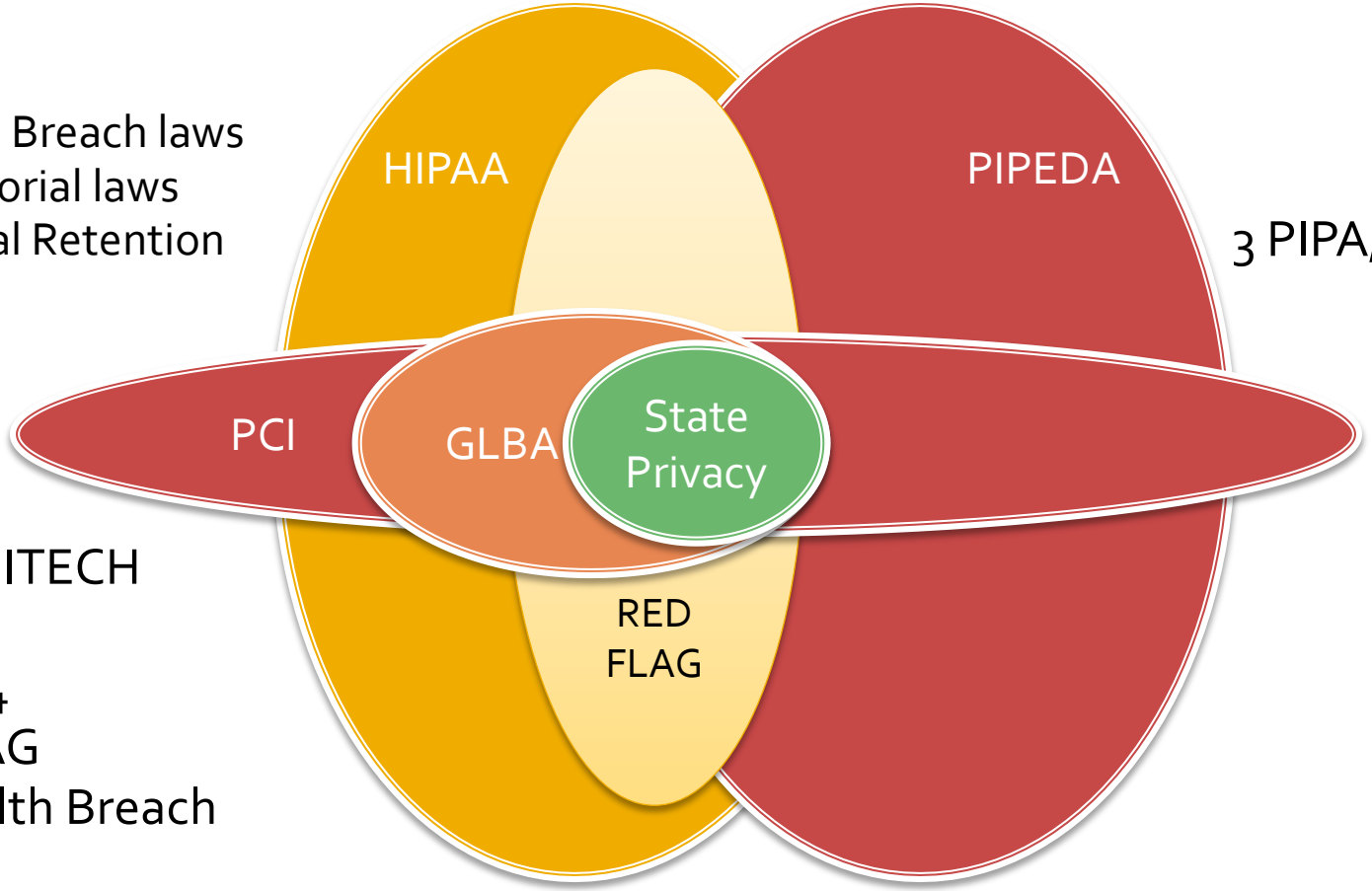
Recommendations



105 Laws and Standards

<u>US</u>
46* State Breach laws
3** Territorial laws
50 Medical Retention
PCI

<u>Canada</u>
PIPEDA
3 PIPA/PPIPS laws



HIPAA/HITECH
GLBA
SOX-404
RED FLAG
FTC Health Breach

- *Texas State law covers the 4 states Alabama, Kentucky, New Mexico, and South Dakota
- ** Territories: Washington DC, Puerto Rico, US Virgin Islands

Next Steps

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 1st, 4th & 5th 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

Final Thoughts

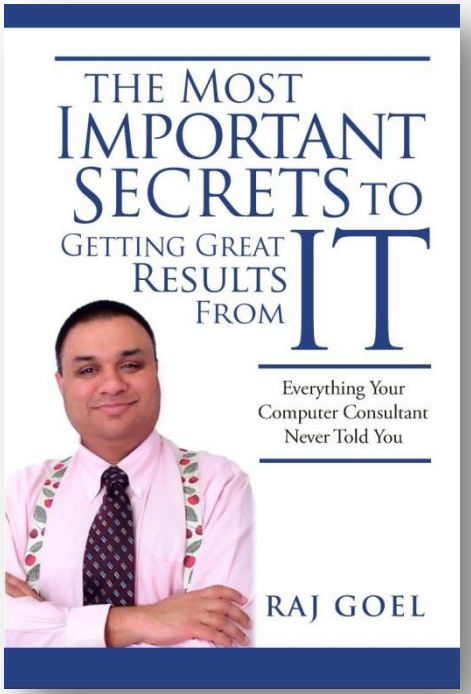
In every generation, a new King John; a new Khruschev and a new Solzhenitsyn is born. It's OUR job as citizens to DEFEND the rights given to us by our respective constitutions and DEMAND that they be conferred on our WEAKEST citizens, not just the strongest or the wealthiest.

Privacy is a human right….not a luxury

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



Author of "The Most Important Secrets To Getting Great Results From IT"
http://www.amazon.com/gp/product/0984424814