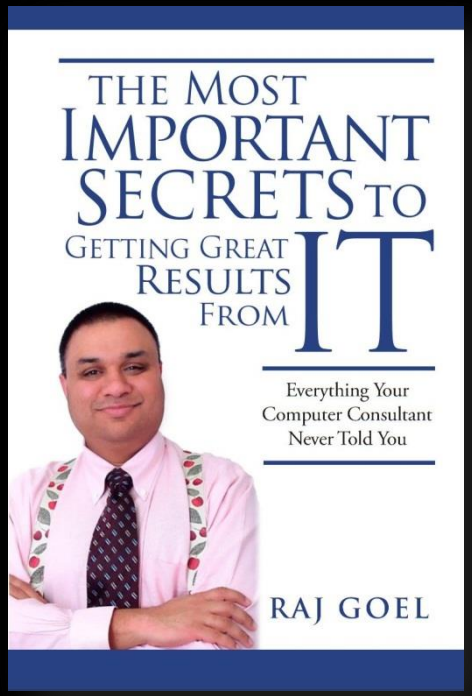
Is Your Company Googling Your Clients' Privacy Away?

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



Raj Goel, CISSP

Raj Goel, CISSP, is an Oracle and Solaris expert and he has over 25 years of experience in software development, systems, networks, communications and security for the financial, banking, insurance, health care and pharmaceutical industries.

Raj is a regular speaker on HIPAA/HITECH, PCI-DSS Credit Card Security, Disaster Recovery, Information Security and other technology and business issues, addressing diverse audiences including technologists, policy-makers, front-line workers and corporate executives.

A internationally known expert, Raj has appeared in over 30 magazine and newspaper articles worldwide, including ***Information Security Magazine***, ***PenTest,*** ***CSOOnline***, ***Entrepreneur Magazine***, ***Business2.0*** *and* ***InformationWeek***, and on television including ***CNNfn,*** ***Geraldo At Large*** and **PBS.**

Raj has presented at:

- **ISC²** conferences
- **ASIS International** conferences
- **BrightTalk** conferences
- Medical Conferences
- Legal Conferences
- **GBATA 2012 (keynote speaker)**
- **The Hague, Netherlands NCSC.NL 2013 (plenary speaker)**

Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

GBATA | Global Business and Technology Association™

CSO
BUSINESS RISK LEADERSHIP

ASIS INTERNATIONAL
Advancing Security Worldwide®

The New York Times

Entrepreneur

(ISC)²
SECURITY TRANSCENDS TECHNOLOGY℠

BrightTALK™

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP®

FOX NEWS Channel

CyberHood Watch

PBS

DIVISION OF HOMELAND SECURITY AND EMERGENCY SERVICES
OFFICE OF COUNTER TERRORISM
NEW YORK STATE



NYIT MAGAZINE

CNNfn
the financial network

PenTest magazine

ITV

NEW YORK COUNTY
NYCLA
LAWYERS' ASSOCIATION

Agenda

- Google's Privacy Policy
- Google Search, Gmail, Trends, etc
- ECPA
- The future is already here
- NSA's PRISM
- Suggestions, Next Steps

Reality…



Google Search – Start of the spider's web…

- Google's cookies do not expire until 2038.
- All of Google's properties (Google, Gmail, Orkut, Google Desktop, etc.) have deep-linked cookies that expire in 2038.
- Each Google cookie has a unique GUID.
- Every time you search, the search queries are tied back to your cookie. Google does not delete anything.
- Google response to John Battelle:
- 1) "Given a list of search terms, can Google produce a list of people who searched for that term, identified by IP address and/or Google cookie value?"
- 2) "Given an IP address or Google cookie value, can Google produce a list of the terms searched by the user of that IP address or cookie value?"
- I put these to Google. To its credit, it rapidly replied that the answer in both cases is "yes."

Google Cookies– the 2-year myth

- Google's cookies do not expire until 2038.
- "Google will start issuing our users cookies that will be set to auto-expire after 2 years, while auto-renewing the cookies of active users during this time period. In other words, users who do not return to Google will have their cookies auto-expire after 2 years. Regular Google users will have their cookies auto-renew, so that their preferences are not lost. And, as always, all users will still be able to control their cookies at any time via their browsers."
- - http://googleblog.blogspot.com/2007/07/cookies-expiring-sooner-to-improve.html
- Translated into English:
- The cookies expire 2 years AFTER complete inactivity.
- If you use Google products/services, the 2 year period restarts NOW!

Gmail – threads merge

- One key risk is that because GMail gets your consent to be more than an e-mail delivery service -- offering searching, storage and shopping -- your mail there may not get the legal protection the ECPA gives you on E-mail.
- The storage of e-mail on 3rd party servers for more than 180 days almost certainly causes the loss of those privileges.
- This in turn creates a danger that we may redefine whether e-mail has the "reasonable expectation of privacy" needed for 4th amendment protection.
- Correlation of search and mail has real risks.
- - Brad Templeton, Chairman of the Electronic Frontier Foundation, http://www.templetons.com/brad/gmail.html

Gmail – threads merge (2)

- Knowing someone is using Gmail because their email address is rajgoel@gmail.com is easy.
- What if your business partner, client or prospect uses raj@stanford.edu or raj@chinatech.com--can YOU tell if it's hosted at Gmail?
- The plans, proposals, research, recommendations, etc. you email out – are they being indexed at google?

Gmail Patents – Weaving the threads

- Patent #20040059712 - “Serving advertisements using information associated with e-mail” allows Google to create profiles based on the following data:
- * Information about the sender, including information derived from previous interactions with the sender
- * Information about the recipient, including information derived from sender's address book or from previous interactions with the sender
- * Information about a recipient based on a profile or information about the sender (the example from that patent is: "Sender is a wine enthusiast and has recently searched for and/or browsed pages related to wine, suggesting that recipient may also be interested in wine")
- * Information from other e-mails sent by sender
- * Information from other e-mails received by recipient
- * Information from other e-mails having the same or similar subject text
- * Information about recipient from sender's contact information
- * Directory and file information based on the path name of attachments sent in previous e-mails (e.g. building an index of filenames on sender or recipient's computer)
- - http://www.epic.org/privacy/gmail/faq.html

Google Alerts

- Google Alerts are email updates of the latest relevant Google results (web, news, etc.) based on your choice of query or topic.

- Is someone at Citibank researching “windpower in India”? “terrorism in Niger Delta”?

- Google knows:
- - who's researching it (GUID/email)
- - How many people are doing it.
- - Popularity of story or search
- - Trend Activity

Chrome

- Chrome is google's browser, based on the Webkit framework.

- Dangers:
- - Google knows every URL you searched (same as every other browser)
- - Google knows every character you type! Even if you don't hit enter
- - Google tracks every “auto suggestion”

- http://coderrr.wordpress.com/2008/09/03/google-chrome-privacy-worse-than-you-think/

Android = New Microsoft

- Android apps security is worse than Windows.
- Free android wall paper app downloaded millions of times. Sends collected user data to China.
- http://www.theregister.co.uk/2010/07/29/suspicious_android_app/
- 20% of tested Android apps allow developers access to sensitive or private data
- http://news.cnet.com/8301-27080_3-20008518-245.html

Android 2013 = Windows95

- The researchers found that two-thirds of the 30 apps in the sample used sensitive data suspiciously, half share location data with advertising or analytics servers without requiring "implicit or explicit user consent," and one-third expose the device ID, sometimes with the phone number and the SIM card serial number. In all, the researchers said they found 68 instances of potential misuse of users' private information across 20 applications.

  http://news.cnet.com/8301-27080_3-20018102-245.html

Flu Trends

- Google Flu Trends: Google automatically analyzes the search queries for "flu", "influenza", etc. Displays charts of aggregate



Google Streetview Password grab

- Google admits to “accidentally” capturing usernames, passwords, emails from open wifi access points.
- “in some instances entire emails and URLs were captured, as well as passwords.“
- - http://googlepublicpolicy.blogspot.com/2010/10/creating-stronger-privacy-controls.html

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

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

ECPA - Disclosure Rules

- Compelled Disclosure Rules in 18 U.S.C. § 2703
- Section 2703 mandates different standards the government must satisfy to compel different types of communications. To compel a provider of ECS to disclose contents of communications in its possession that are in temporary "electronic storage" for 180 days or less, the government must obtain a search warrant.67 To compel a provider of ECS to disclose contents in electronic storage for greater than 180 days or to compel a provider of RCS to disclose contents, the government has three options.
- First, the government can obtain a search warrant.
- Alternatively,investigators can use less process than a warrant, as long as they combine that process with prior notice.
- Specifically, the government can use either a subpoena or a "specific and articulable facts" court order pursuant to 18U.S.C. § 2703(d), combined with prior notice to the "subscriber or customer" (which can be delayed in some circumstances).73 The court order found in § 2703(d), often referred to as a "2703(d)" order or simply a "d" order, is something like a mix between a subpoena and a search warrant. To obtain the order, the government must provide "specific and articulable facts showing that there are reasonable grounds to believe" that the information to be compelled is "relevant and material to an ongoing criminal investigation."74 If the judge finds that the factual showing has been made, the judge signs the order. The order is then served like an ordinary subpoena; investigators bring or fax the order to the ISP, and the ISP complies by turning over the information to the investigators.
- - http://papers.ssrn.com/sol3/papers.cfm?abstract_id=421860
- Professor Orin Kerr, George Washington University - Law School
- TRANSLATION:
- After 180 days, Government access to your Gmail, Hotmail, Yahoo Mail, etc. becomes significantly easier.

ECPA & You

- CSO's and CPOs should know about ECPA
- Employees are forwarding emails to GMAIL because it is fast, easy to use and has copious capacity. The opposite of most corporate email systems.
- How many of your employees are forwarding emails to gmail/yahoo/hotmail right now?

US vs WARSHAK

- US Gov't claims:
- “users of ISPs don't have a reasonable expectation of privacy”
- “Many employees are provided with e-mail and Internet services by their employers. …[Court] orders directed to the email of employees who have waived any possible expectation of privacy do not violate the Fourth Amendment.”
- "some email accounts are abandoned, as when an account holder stops paying for the service [or dies] and the account is cancelled." There "can be no reasonable expectation of privacy in such accounts.
- “… hackers may obtain internet services and email accounts using stolen credit cards. Hackers maintain no reasonable expectation of privacy in such accounts.”
- - http://www.theregister.com/2007/11/04/4th-amendment_email_privacy/

- So, Where's your email hosted? Do the TOS' specify privacy and ownership? What about your clients, partners or vendors?

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/

©2013 Raj Goel / Raj Goel, CISSP / raj@brainlink.com / 917-685-7731

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

©2013 Raj Goel / Raj Goel, CISSP / raj@brainlink.com / 917-685-7731

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/

©2013 Raj Goel / Raj Goel, CISSP / raj@brainlink.com / 917-685-7731

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/

Google's Double Irish Dutch Sandwich

- Google uses a legal tax dodge called the "Double Irish" and "Dutch Sandwich" to avoid $ 1 BILLION in taxes per year.
- Their effective tax rate is 2.4%
  - http://nymag.com/daily/intel/2010/10/google_uses_the_double_irish_a.html
- Google: "**Don't be evil. That's our job**"

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.

EZPass outs cheaters in divorce court

- Adulterers, beware: Your cheatin' heart might be exposed by E-ZPass.
- E-ZPass and other electronic toll collection systems are emerging as a powerful means of proving infidelity. That's because when your spouse doesn't know where you've been, E-ZPass does.
- "E-ZPass is an E-ZPass to go directly to divorce court, because it's an easy way to show you took the off-ramp to adultery," said Jacalyn Barnett, a New York divorce lawyer who has used E-ZPass records a few times.
- Lynne Gold-Bikin, a Pennsylvania divorce lawyer, said E-ZPass helped prove a client's husband was being unfaithful: "He claimed he was in a business meeting in Pennsylvania. And I had records to show he went to New Jersey that night."

- - http://www.msnbc.msn.com/id/20216302/

Ezpass manufacturer files patent for INWARD facing Camera

- Kapsch Traffic Com AG, a transponder (i.e., E-Z Pass and IPass) manufacturer, filed a patent for technology to include an inward and outward pointing camera.

- MSNBC reports that Kapsch TrafficCom AG, an Austrian company that creates transponders like E-Z Pass, which allows cars to breeze through tolls, filed a patent for technology that would include cameras in such devices. Cameras would point inside the car as well as out.

- - http://www.theblaze.com/stories/could-your-freeway-pass-soon-contain-a-camera-that-films-you/

Vendors "expand the truth"

- "Dropbox employees aren't able to access user files".
- BoingBoing.net, "Dropbox's new security policy implies that they lied about privacy from the start"

- http://boingboing.net/2011/04/25/dropbox-cto-on-their.html

- "DROPBOX: We'll turn your files over to the government if they ask us to"

- - Business Insider, http://www.businessinsider.com/dropbox-updates-security-terms-of-service-to-say-it-can-decrpyt-files-if-the-government-asks-it-to-2011-4

Cloud developers are developers…

- Dropbox's security hole lets others access your Dropbox account without your knowledge.
- Newton's concept, tested on a Windows machine, uses Dropbox's own configuration files; configuration data, file/directory listings, hashes which are stored in numerous SQLite database files located in %APPDATA%\Dropbox. Inside one file lies a database row containing a users "host_id", which is used to authenticate each individual user.
- Modifying this file and changing the host_id to that of another Dropbox user automatically authenticates the account, providing complete access to that person Dropbox…
  - - http://thenextweb.com/industry/2011/04/08/dropbox-security-hole-could-let-others-access-your-files/

©2011 Raj Goel

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/

©2011 Raj Goel

State Of Security in a nutshell





A look at how Las Vegas slots and electronic voting machines compare:

	LAS VEGAS SLOTS	ELECTRONIC VOTING MACHINES
Software	State of Nevada has access to all software. Illegal to use software that is not on file.	Software is a trade secret.
Spot-Checking	State gaming inspectors show up unannounced at casinos to compare computer chips with those on file. If there is a discrepancy, the machine is shut down and investigated.	No checks are required. Election officials have no chip to compare with the one found in the machine.
Background Scrutiny	Manufacturers subjected to background checks. Employees are investigated for criminal records.	Citizens have no way of knowing, for example, whether programmers have been convicted of fraud.
Equipment Certification	By a public agency at arm's length from manufacturers. Public questions invited.	By for-profit companies chosen and paid by the manufacturers. No public information on how the testing is done.
Handling Disputes	Casino must contact the Gaming Control Board, which has investigators on call round the clock. They can open up machines to inspect internal mechanisms and records of recent gambling outcomes.	In most cases, a voter's only recourse is to call a number at the board of elections that may or may not work to lodge a complaint that may or may not be investigated.

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

- William Gibson, Author, futurist

©2013 Raj Goel / Raj Goel, CISSP / raj@brainlink.com / 917-685-7731

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

©2013 Raj Goel / Raj Goel, CISSP / raj@brainlink.com / 917-685-7731

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/

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

©2013 Raj Goel / Raj Goel, CISSP / raj@brainlink.com / 917-685-7731

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

©2013 Raj Goel / Raj Goel, CISSP / raj@brainlink.com / 917-685-7731

PRISM – How & What

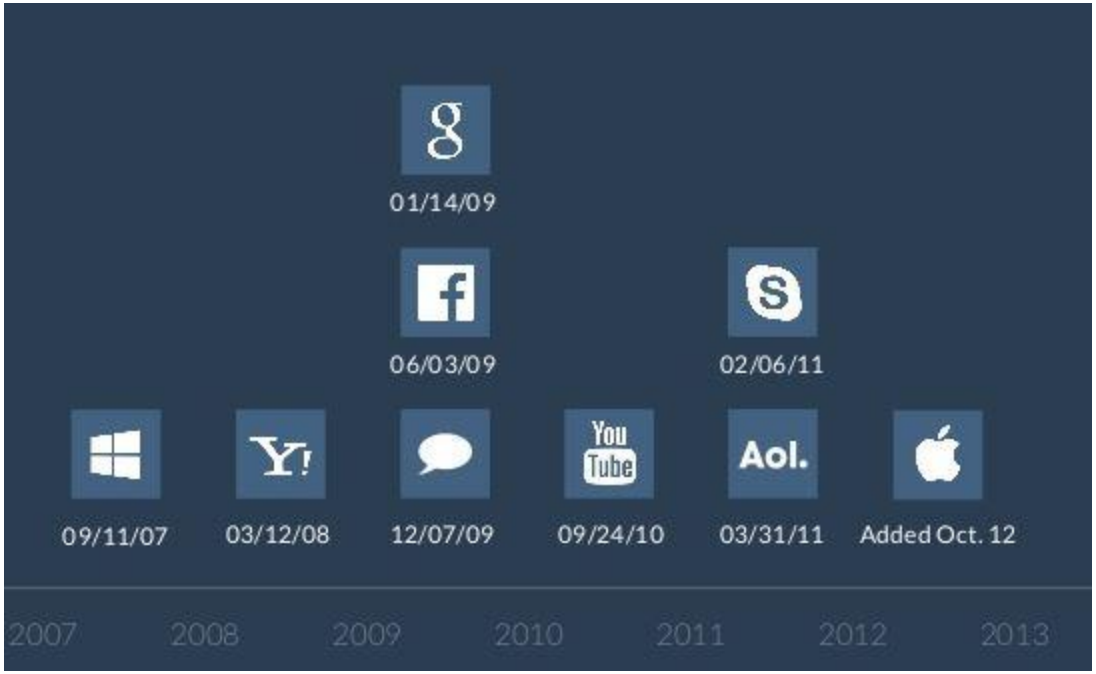




http://fr.slideshare.net/EmilandDC/dear-nsa-let-me-take-care-ou

PRISM – The Players





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

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

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/

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

Sites to Bookmark

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

©2013 Raj Goel / Raj Goel, CISSP / raj@brainlink.com / 917-685-7731

Eric Schmidt on Privacy

- We know where you are. We know where you've been. We can more or less know what you're thinking about."
- "If you have something that you don't want anyone to know maybe you shouldn't be doing it in the first place"
- "Streetview the cars we drive only once, you can just move, right?"
- "Just remember when you post something, the computers remember forever"
- "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.
- "Tell your kids on their third birthday, 'We will always know your password until you're 18.' Tell them again on their fourth birthday, on their fifth birthday." By the time they're 13 Schmidt argues, they'll accept it.
- You have to fight for your privacy or you will lose it

©2013 Raj Goel / Raj Goel, CISSP / raj@brainlink.com / 917-685-7731

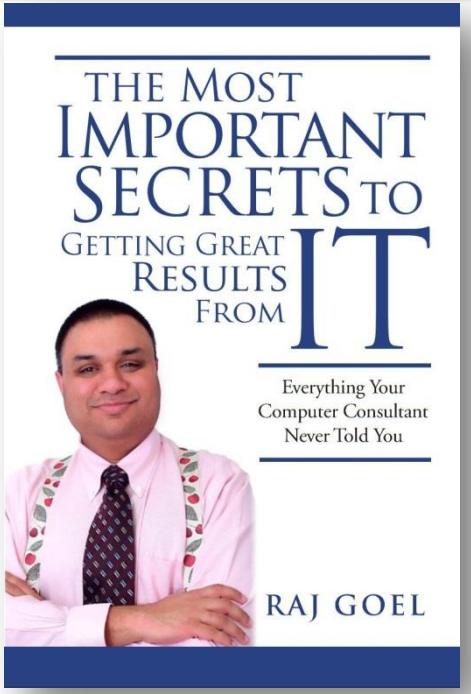
Final Thoughts

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
3. Review your foreign travel technology plans
4. JOIN the EFF
5. Analyze trends and pay attention to regulatory changes and legal opinions
6. Keep on top of emerging threats
7. Perform in-depth information flow analysis, information leakage analysis.

- **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