brainlink

You run your business and leave the IT audits to us.

A Global Perspective on Mobile Security, Privacy and Safety

Raj Goel, CISSP

Chief Technology Officer

Brainlink International, Inc.

raj@brainlink.com / 917-685-7731

First Cloud Application?

- Voicemail
- Similarities to clouds today
- What have we learned from the history of Voicemail that might apply to clouds?

- Where is your voicemail stored?
- Do you know? Do you care?
- Do you TRUST your provider?
- Should You?

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.

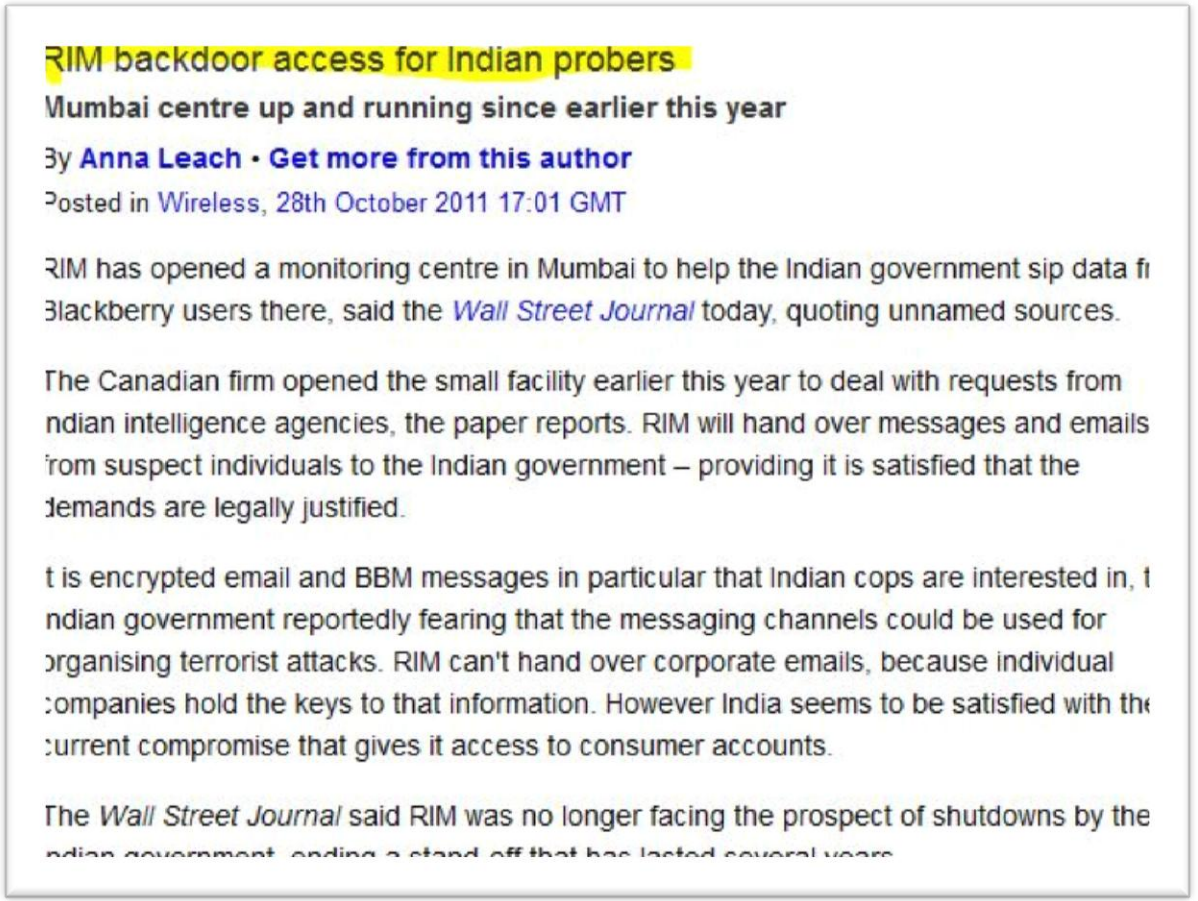
But unlike the Arab spring protests, which used the very public social media forums Facebook and Twitter to rally the troops, BlackBerry's version of IM was the favoured mode in the capital according to anecdotal evidence.

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/

New India Law requires providers to provide realtime location of cell phones

The Indian government is looking to track all mobile phone users.

By 2013, at least 60 per cent of the calls in urban areas would have to be accurately tracked when made 100 metres away from the nearest cell tower. By 2014, the government will seek to increase the proportion to 75 per cent in cities and 50 per cent in suburban and rural areas.
For calls made 300 metres from the nearest cell tower, accurate coordinates will be required for 95 per cent in cities and 60 per cent in towns and villages at the end of two years.

http://www.indianexpress.com/news/soon-govt-will-keep-track-of-where-every-mobile-phone-user-is/912681/

Germany's Intelligence failed to detect Neo-Nazi gang. Too busy spying on former East Germans

GERMANY'S intelligence services failed to detect a gang of neo-Nazis who murdered ten people over several years. Never mind. They have a vice-president of the Bundestag in their sights.

the spooks were busy watching the Left Party, the fourth-largest in the Bundestag. The federal office is monitoring 27 of its deputies, including Petra Pau (a Bundestag vice-president) and a member of the committee that oversees the intelligence services. The party, or affiliated groups, are also targets in most states. This constitutes "defamation of the opposition", complained Jan Korte, a legislator on the watch list.

There are reasons to keep an eye on the Left Party. It is the direct descendant of East Germany's communists and expanded westward by attracting disgruntled Social Democrats. Although the party espouses "democratic socialism" it harbours some groups that seem unsure about democracy. It has seats in 13 state legislatures and has helped govern, mostly pragmatically, three eastern states. The federal agency has been watching it since 1995.

http://www.economist.com/node/21546060

Australian Police spy on email, web usage without warrants

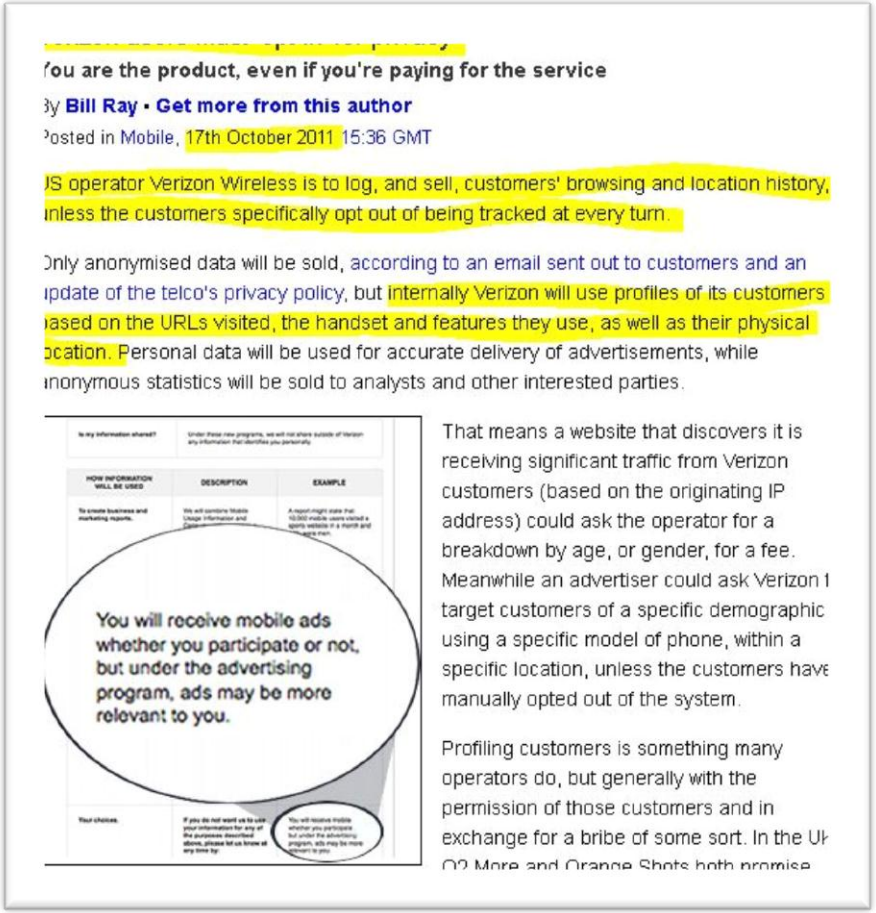
Scott Ludlam, Greens senator … “We’ve already taken some pretty dangerous steps … towards the surveillance state.”

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

Verizon Wireless to sell Customer Data



'ou are the product, even if you're paying for the service

By **Bill Ray** • **Get more from this author**

Posted in Mobile, 17th October 2011 15:36 GMT

JS operator Verizon Wireless is to log, and sell, customers' browsing and location history, inless the customers specifically opt out of being tracked at every turn.

Only anonymised data will be sold, according to an email sent out to customers and an update of the telco's privacy policy, but internally Verizon will use profiles of its customers based on the URLs visited, the handset and features they use, as well as their physical location. Personal data will be used for accurate delivery of advertisements, while anonymous statistics will be sold to analysts and other interested parties.

That means a website that discovers it is receiving significant traffic from Verizon customers (based on the originating IP address) could ask the operator for a breakdown by age, or gender, for a fee. Meanwhile an advertiser could ask Verizon t target customers of a specific demographic using a specific model of phone, within a specific location, unless the customers have manually opted out of the system.

Profiling customers is something many operators do, but generally with the permission of those customers and in exchange for a bribe of some sort. In the UK O2 More and Orange Shots both promise

http://www.theregister.co.uk/2011/10/17/verizon_privacy/

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 purpose**s.

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

Orkut – Brazil & India

Google has designed a special Orkut admin tool for deleting or blocking illegal content, and given Brazilian police access to this tool. This means that if you're on Orkut and you say something that in Brazil could be considered illegal (such as celebrity gossip, Consumerist-style corporate bashing, mistreating animals), the Brazilian police can censor the community where this "illegal" speech is seen.

- boingboing.net

Never mind the bat signal - cops in India have been equipped with a sort of “red phone” e-mail address at Google. The search engine giant, according to various Indian sources, wants to help put a stop to hate speech and other objectionable content that’s been showing up on Orkut.

Onstar – Subscribers still at risk

If you're a current OnStar subscriber, however, your data's still being mined, like it or not. According to **the company's terms of service**, subsection 33 (titled "YOUR PRIVACY"):

> *The information we may get from your Car includes things such as: data about its operation; data about your use of the OnStar Services; the location of your Car; data about accidents involving your Car, including safety belt usage; and information about your use of the Car and its features. We may also approximate the speed of your Car based on GPS data to support a limited number of OnStarServices, such as Stolen Vehicle Assistance services, as further described in our Privacy Statement. We may collect information from your Car on a periodic or regular basis.*

http://techland.time.com/2011/09/28/onstar-reverses-position-wont-track-you-if-you-cancel-service/

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/

Big Brother Is Watching: Document Reveals Surveillance of Social Media, Blogs, Image-Sharing Sites

By GRAEME MCMILLAN | @graememm | January 12, 2012 | 16

JIM URQUHART / REUTERS

Hope you're not shy, because there's a good chance you're being watched by the U.S. Department of Homeland Security. According to a government document, the DHS has been monitoring social media as well as select blogs and message boards for more than a year.

The "privacy compliance review" obtained by Reuters comes from last November, but apparently this surveillance has been ongoing since at least June 2010. According to the document, it's designed to "collect information used in providing situational awareness and establishing a common operating picture" with "data published via social media sites [used] solely to provide more accurate situational awareness, a more complete common operating pictures, and more timely information for decision makers." In other words, the DHS is using the Internet to find out what's happening, same as everyone else, but it certainly *sounds* more disturbing.

http://techland.time.com/2012/01/12/big-brother-is-watching-document-reveals-surveillance-of-social-media-blogs-image-sharing-sites/

Privacy Advocates Sue DHS for Big Bro Fake 'Friends' Monitoring Social Media

Privacy advocates are suing DHS for 'covert' social networking surveillance on Facebook and Twitter. EPIC's FOIA lawsuit is a result of Homeland Security refusing to turn over details about Big Brother setting up fake accounts to 'friend' you and better monitor your social media activities.

By Ms. Smith on Thu, 12/22/11 - 12:28pm.

4 Comments Print

Yes, Virginia, Big Brother is watching you in social media and storing those "naughty" tweets, posts and comments. After those hot keyword terms put you on the naughty list, unlike Santa's list, it's not a redo in a year . . . that info will be stored for five years. The EFF previously warned Big Brother wants to be your online buddy on social networking sites. Then the Electronic Privacy Information Center (EPIC) filed a Freedom of Information Act (FOIA) request asking Homeland Security for more details about the agency's plans to setup fake profiles and monitor social media users; but when no documents were produced, EPIC is now suing DHS over 'covert surveillance on Facebook and Twitter.'

Hackers belonging to Anonymous kindly shared with the public such "chumming and baiting" tactics as were disclosed in Aaron Barr's leaked emails.Those sock puppet accounts will try to befriend you, monitor for specific NOC terms, and then collect your PII (personally identifiable information) which will be stored for five years. Many users have a nasty habit of over-sharing on social media even though all that personal or sensitive information is potential fodder for social engineers. EPIC's lawsuit [PDF] against DHS states, "Social media users have no reason to believe that the Department of Homeland Security is tracking their every post." The DHS program plans to share this PII by "email and telephone" with "federal, state, local, tribal, territorial, foreign, or international government partners."

http://www.networkworld.com/community/blog/privacy-advocates-sue-dhs-covert-surveillance-big-bro-fake-friends-monitoring-social-media

Ubiquitous Surveillance from Big Brother's WAYBACK Machine

As the price of digital storage drops and the technology to tap electronic communication improves, authoritarian governments will soon be able to perform retroactive surveillance on anyone within their borders, according to a Brookings Institute report.

These regimes will store every phone call, instant message, email, social media interaction, text message, movements of people and vehicles and public surveillance video and mine it at their leisure, according to "Recording Everything: Digital Storage as an Enabler of Authoritarian Government," written by John Villaseno, a senior fellow at Brookings and a professor of electrical engineering at UCLA.

That will enable shadowing people's movements and communications that took place before the individuals became suspects, he says.

"For example, if an anti-regime demonstrator previously unknown to security services is arrested, it will be possible to go back in time to scrutinize the demonstrator's phone conversations, automobile travels, and the people he or she met in the months and even years leading up to the arrest," the report says.

- http://www.networkworld.com/news/2011/121511-government-surveillance-254137.html

FourSquare, Facebook Places, etc.

- UK Ministry of Defense (MoD) warns that Facebook Places (which is enabled by default!) provides a targeting pack for terrorists.

- "The main concern relating to the use of the application, is that it may inadvertently compromise the locality of a military user," the document says."

http://www.theregister.co.uk/2010/10/01/mod_facebook_places/

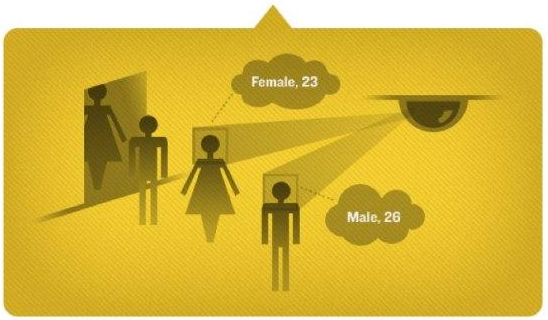
Girls Around Me

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/

Mercedes Benz updates car software remotely

This new system upgrades on the fly, he said, the first such in-car application to do so. “It’s seamless to the customer,” Link said. “I have a friend who was excited about his system upgrade, which required him to plug in his stick and leave his car running for 45 minutes. Who wants to do that? In a process called ‘reflashing,’ the Mercedes system can turn on the car operating system (CU), download the new application, then cut itself off. It doesn’t require you to do anything at all.”

The implications of this go far beyond transparent upgrade of your streaming music system. Consider that the average car has 70 to 100 electronic control units (ECUs) and even econoboxes have lines of code in the tens of millions — the Mercedes S-Class has more than 20 million. According to Link, software-related recalls are a big problem for carmakers, costing $75 to $95 per car. Not only is it expensive, but it’s a hassle for drivers—nobody likes bringing their car to the shop.

- http://www.txchnologist.com/2012/new-york-auto-show-upgrading-auto-software-in-a-flash

Thieves steal BMWs in 3 minutes

There has been an unusual spike in the number of BMWs stolen in the UK this year, with some sources suggesting the number may be 300 cars or higher. The cars are being stolen without activating car alarms or immobilizers.

The suspected method involves the use of devices that plug into the car's OBD port and can program blank key fobs, leaving owners with keys to missing cars.

The essential theft process varies in detail, but all reports seem to have a fundamental methodology in common. First, the car is entered, either via nearby RF jammers that block the fob lock signal from reaching the car (preventing owners from securing their vehicles) or, more crudely, by breaking a window, as seen in the video in this post of the 1 Series being stolen. In cases of the window break, the thieves seem to be exploiting a gap in the car's internal ultrasonic sensor system to avoid tripping the alarm.

- http://www.technolog.msnbc.msn.com/technology/technolog/hackers-steal-bmws-3-minutes-using-security-loophole-868400

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/

NYTimes – Leave your laptop, cell at home when travelling abroad

When Kenneth G. Lieberthal, a China expert at the Brookings Institution, travels to that country, he follows a routine that seems straight from a spy film. He leaves his cellphone and laptop at home and instead brings "loaner" devices, which he erases before he leaves the United States and wipes clean the minute he returns. In China, he disables Bluetooth and Wi-Fi, never lets his phone out of his sight and, in meetings, not only turns off his phone but also removes the battery, for fear his microphone could be turned on remotely. He connects to the Internet only through an encrypted, password-protected channel, and copies and pastes his password from a USB thumb drive. He never types in a password directly, because, he said, "the Chinese are very good at installing key-logging software on your laptop.

- http://www.nytimes.com/2012/02/11/technology/electronic-security-a-worry-in-an-age-of-digital-espionage.html?pagewanted=all

Times Square Marriott Injects Javascript to break privacy and serve Ads

Marriott is injecting JavaScript into the HTML of every webpage its hotel customers view for the purpose of injecting ads and in the meantime, breaking YouTube. Marriott's wireless internet service provider is a third-party company called Hotel Internet Services, so it is possible, though unlikely, that Marriott doesn't know what's going on. But it's crazy to me that I'm paying $368 a night for a hotel room, and this is how I get treated.Update: I guess not all press is good press. Ronen Isaac coincidentally of Wlan Mall appears to have taken down the Vimeo video above that did such an excellent job describing how the Revenue eXtraction Gateway worked

- http://justinsomnia.org/2012/04/hotel-wifi-javascript-injection/

BYOD Blowback drives more IT underground

Enterprises unnerved by the bring-your-own-device movement in which they encouraged employees to use personal devices at work, are now angering workers by trying to lock down those very devices.According to new research from Forrester, the unintended, but entirely predictable, consequence is that many of those frustrated employees just turn to new, unsanctioned devices instead.After surveying 5,102 business users for its “Five Steps to a Successful BYOC Program” Forrester prefers the term “computer” to “device”, here’s what Forrester has to say: Today’s workers often need more than the locked-down corporate PC’s and are spending an average of $1,253 annually of their own money on computers to do their jobs. … Yet the same survey reveals that only 12% of firms encourage those who do so, with the rest actively discouraging it – and some even penalizing employees. The mismatch between employee needs and IT’s position is obvious, but few organizations are adequately prepared to change course.The examples of this tactic are piling up. IBM, for example, disables Siri in employees’ iPhones and forbids the use of Dropbox, the wildly popular cloud-based file storage, sync and sharing service. That raises interesting questions in the cloud computing era, where users can tap consumer-oriented services from their personal phones and laptops that may be verboten in the corporate context.

- http://gigaom.com/cloud/byod-blowback-drives-more-it-underground/

BYOD – Japan - Winny

- “in particular, a military agency was forced to admit that classified information from the Maritime Self Defence Force was uploaded by a computer with winny software installed on it.
- Following this, ANA (All Nippon Airlines) were also the victims of an embarrassing data leak, with passwords for security-access areas in 29 airports across Japan being leaked over the program. This follows a similar incident from JAL Airlines on 17th December 2005, after a virus originating from Winny affected the computer of a co-pilot.
- Arguably the biggest winny-related leak however, is that of the Okayama Prefectural Police Force, whose computer leaked data on around 1,500 investigations. This information included sensitive data; such as the names of sex crime victims, and is the largest amount of information held by Japanese police to have ever leaked online.”
- - WikiPedia - http://en.wikipedia.org/wiki/Winny

HISTORY & REGULATIONS

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/

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

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?

ECPA - Electronic Communications Privacy Act (1986)

- **FBI Abuses Patriot Act**

http://www.nytimes.com/2007/03/10/washington/10fbi.html

- **Sprint received 8 MILLION law enforcement requests in 13 months**

http://www.eff.org/deeplinks/2009/12/surveillance-shocker-sprint-received-8-million-law

- **Your Identity for Sale**

http://money.cnn.com/2005/05/09/pf/security_info_profit/index.htm

- **Google "FBI buys data from private sector"**

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/

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

Next Steps

If you have any questions about this presentation, or any other topic, feel free to contact me.

Professionally, I'm available to speak at Bar Associations (CLE), CPA Societies (CPE), and Conferences.

If you'd like to educate the kids, interns & college students in your life about the dangers of social media, share this video with them:

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

Self-Promo

At Brainlink, We provide IT/Computer Consulting for Small Businesses in New York City.

Across the USA, I personally provide

- COMMON SENSE BASED IT Security and Privacy Breach law compliance audits (HIPAA/HITECH, PCI-DSS)
- Information Security Audits
- IT Consulting for Healthcare

If you like what you're hearing, hire me!

www.RajGoel.com

Contact Information

Raj Goel, CISSP

Chief Technology Officer

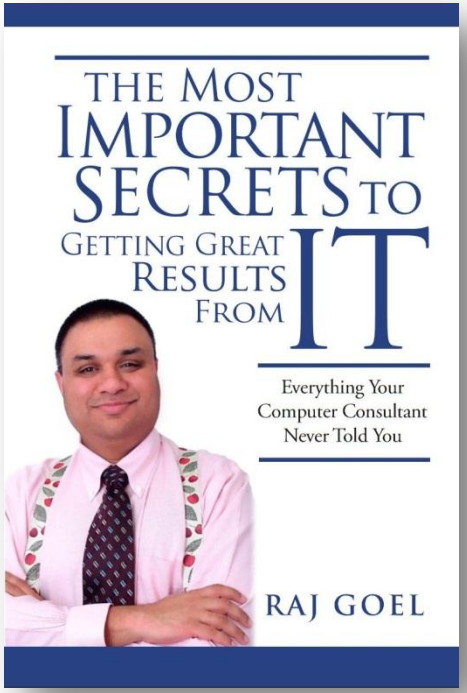
Brainlink International, Inc.

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