



Social Media & Cloud Computing Threats to Privacy, Security & Liberty

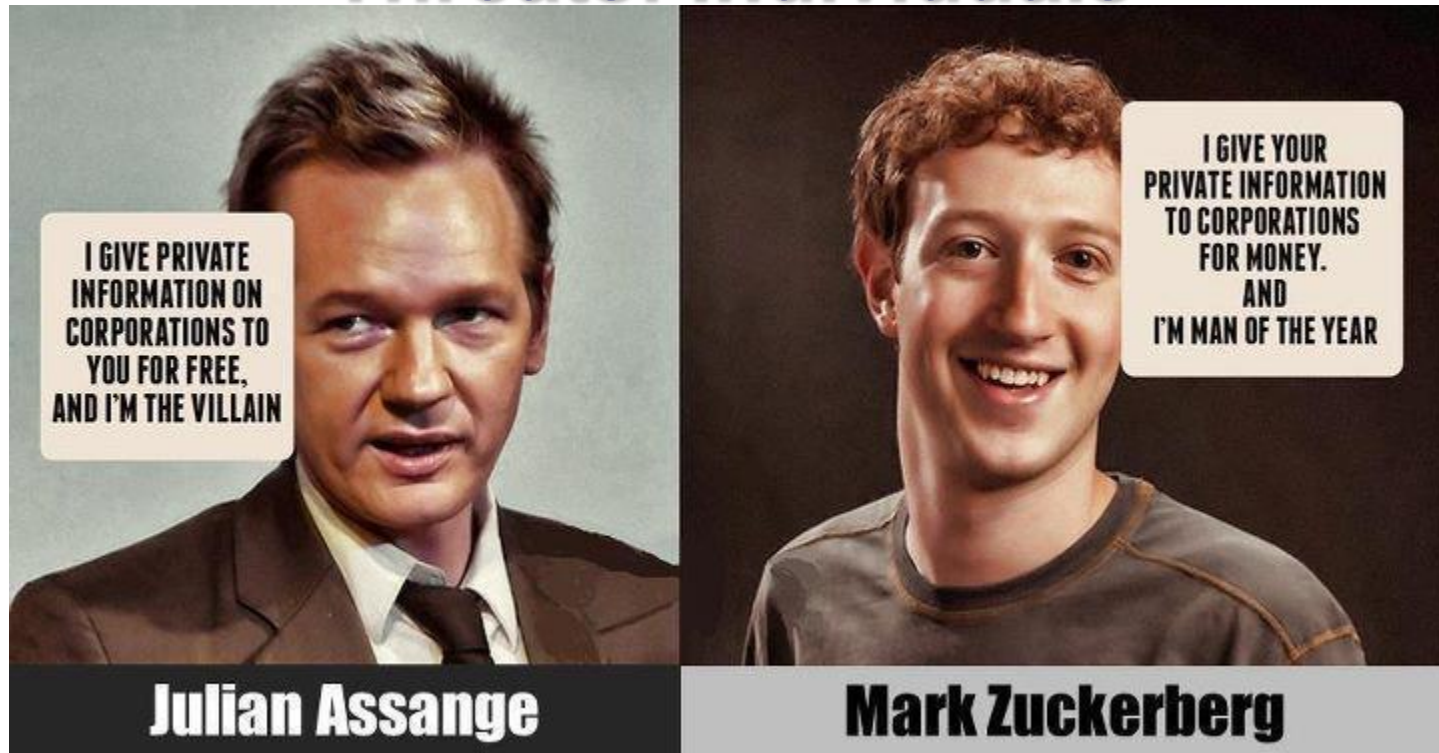
Raj Goel, CISSP

Date



NEW YORK INSTITUTE OF TECHNOLOGY

Threats: Individuals



College Admissions

Social-networking sites viewed by admissions officers

Survey shows some use Facebook, MySpace as another aspect to college application

September 20, 2008 | By Emma Graves Fitzsimmons and Bonnie Miller Rubin

High schoolers say getting into college is no longer only about sky-high test scores and impressive extracurricular activities. Now it means being smart about their online personas as well.

In a new survey, 10 percent of admissions officers from prestigious schools said they had peeked at sites like Facebook and MySpace to evaluate college-bound seniors. Of those using the profiles, 38 percent said it had a "negative impact" on the applicant, according to Kaplan Inc., the education services company that polled the officers.

At least one admissions officer had rescinded an offer because of an applicant's postings, results showed. The survey went out to 500 schools -- of which 320 responded -- in July and August and promised anonymity.

http://articles.chicagotribune.com/2008-09-20/news/0809190659_1_social-networking-sites-admissions-facebook-profile

College Ejection

What you say online could haunt you

by Janet Kornblum and Mary Beth Marklein, **USATODAY**

College student Michael Guinn thought the photos he posted of himself dressed in drag would be seen only by friends. But he made a mistake. And when someone showed the photos on [facebook](#) to administrators at John Brown University, a Christian college in Siloam Springs, Ark., it was "the last straw for them," says Guinn, 22, who is gay.

Sign up to receive
e-newsletter a
news, Hot Site:

E-mail:

Select



Be careful
what you post:
Students are
getting expelled
for what they
post on social
websites.

Facebook.com

In January, he was kicked out of school, his virtual paper trail of musings about boyfriend and visits to clubs a clear sign to administrators that, despite repeated warnings, Guinn's activities were in violation of campus conduct codes stating that students must "affirm and honor Scripture."

http://www.usatoday.com/tech/news/internetprivacy/2006-03-08-facebook-myspace_x.htm

Degree Revocation

SOCIAL NETWORK PROFILE COSTS WOMAN COLLEGE DEGREE

by Sarah Perez / December 5, 2008 6:05 AM / 33 Comments

Tweet 0

Recommend 55

Share

+1 0

Share

This photo is
currently
unavailable

flickr

Forget losing your job, apparently your MySpace or Facebook profile and photos can now cause you to lose your degree. In what may be one of the most frightening rulings regarding social networks and privacy to date, a federal judge has ruled against a former student of Millersville University of Pennsylvania who was denied her college degree because of an unseemly online photo and its accompanying caption found on her social network profile.

The Case of "Drunken Pirate," Stacy Snyder

The woman, Stacy Snyder, sued Millersville in 2007. Snyder was student-teaching at a high school, but had received poor evaluations regarding her professionalism in the classroom. Before her semester-long teaching assignment was up, she was barred from campus. However, it was not the negative reviews that caused her to be barred nor were they responsible for the loss of her degree. It was a MySpace photo.

In the photo, Snyder was posed standing with a cocktail. The caption read "drunken pirate." It was accompanied by a note which made reference to her supervising teacher. That led to the school's decision to end her assignment, which in turn meant she now no longer qualified for her bachelor's degree in education.

http://www.readwriteweb.com/archives/social_network_profile_costs_woman_college_degree.php

Facebook of the nation...

- ▶ Facebook allows developers access to user's full profile.
- ▶ Every time you choose to add an application, Facebook asks you to confirm that you want to let this program both know who you are and access your information. It's impossible for anyone to add any application without agreeing to this set of terms. Once you click okay, that application can technically access quite a bit of public and private profile information.
- ▶ While all of the most private information (like your passwords and e-mail addresses) are kept on Facebook servers and require security authentication, a lot of info is available to applications you add.

According to Facebook's Developers Terms of Use, this can include

". . . your name, your profile picture, your birthday, your hometown location, your current location, your political views, your activities, your interests, your relationship status, your dating interests, your relationship interests, your summer plans, your Facebook user network affiliations, your education history, your work history, copies of photos in your Facebook Site photo albums, and a list of user IDs mapped to your Facebook friends."

- <http://www.removeadware.com.au/articles/facebook-privacy-hackers/>

Lose Your Job – 2003 Michael Hanscom

Even Microsoft wants G5s

Published:
October 23, 2003 – 10:34 pm

Author:
By Michael Hanscom

Categories:


- 15Minutes
- Apple
- Microsoft

Comments:

- 442 Comments
- Comments RSS Feed
- Post a comment

UPDATE: Please take the time to read my followup post, [Fifteen Minutes of Fame](#), for my thoughts on what happened after I posted this picture, why it happened – and most importantly, why I don't blame Microsoft for their actions. Thanks!

It looks like somebody over in Microsoft land is getting some new toys...



I took this shot on the way into work on the loading dock (MSCopy, the print shop I work in, is in the same building as MS's shipping and receiving). Three

<http://www.michaelhanscom.com/eclecticism/2003/10/23/even-microsoft-wants-g5s/>

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 finds 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>

New Zealand Bank Error Fugitives Foiled By Facebook Status Update

By Laura Northrup on May 25, 2009 11:11 AM



—>You know how it goes. You go out and have too many beers, then post a Facebook update with a bit too much information about your evening. Maybe you take it down once you sober up the next day, but not before the damage is done.

Then, if you're Aroha Hurring of New Zealand, Interpol uses your status update to track down you, your sister, her boyfriend, and the

millions of dollars his bank mistakenly deposited in his account.

Last week, Consumerist brought you the story of the struggling gas station owners who were the recipients of a \$10,000,000 NZD bank error, then wired the money out of the country and hadn't been heard from since.

“

Rotorua service station owners Leo Gao and his girlfriend Cara Young fled New Zealand with about \$NZ3 million after they discovered the money in their bank account.

But their chances of being caught have increased after they were joined overseas by Ms. Young's sister, Aroha Hurring, who posted details about their location on her Facebook page.

<http://consumerist.com/2009/05/new-zealand-bank-error-fugitives-foiled-by-facebook-status-update.html>

Facebook photo blunder leads to mafia arrest in Marbella

AUGUST 26, 2011 • ANDALUCIA, LEAD, MALAGA • 2 COMMENTS

★★★★★ (2 votes, average: 4.50 out of 5)



A MEMBER of the Italian Mafia – who had been on the run for almost 10 years – has been arrested in Marbella after his ‘stupid’ girlfriend posted pictures of the couple on Facebook.

One of Italy’s most-wanted, Salvatore D’Avino, 39, was caught out after detectives spotted photos on the social networking site of his pregnant girlfriend Brada Hint, 31,

standing in front of the upmarket Nikki Beach Club.

Italian police alerted the Spanish authorities who then traced the couple to their Costa del Sol hideout and arrested D’Avino who is said to be a member of the Giuliano clan, of the notorious Camorra mafia in Naples.

He was listed on the Italian police’s top 100 most wanted after police issued two arrest warrants for D’Avino in 2003 and 2007 on drug trafficking and mafia charges.

D’Avino – who was believed to have been hiding in Morocco for years – is also accused of being part of a plot to flood Marbella with more than 250,000 Ecstasy tablets.

Marshall Angelo Mazzagatti, of the Naples police who led the operation said: “He couldn’t believe it when police arrived and arrested him. He thought after nearly a decade on the run he was home free.

<http://www.theolivepress.es/spain-news/2011/08/26/facebook-photo-blunder-leads-to-mafia-arrest-in-marbella/>

N.C. Man's Facebook Photo Leads to Arrest

September 29, 2011 1:07 PM

Share this


 Like

 Tweet


0

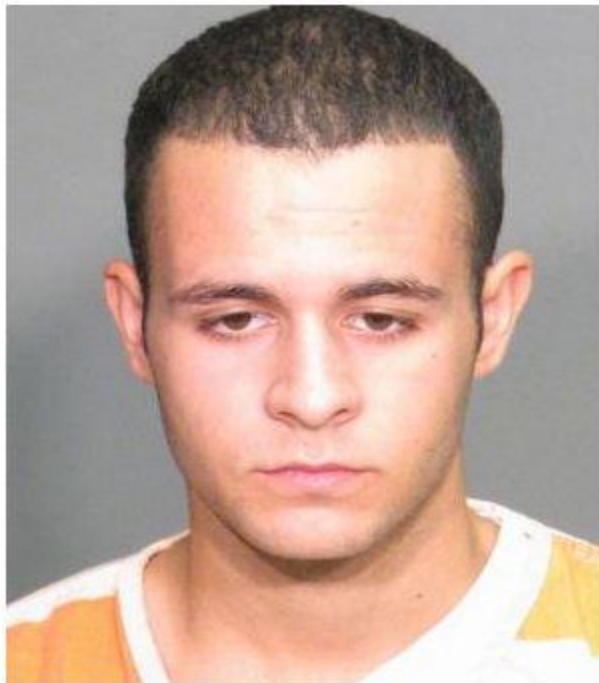
 +1

0

 Share

1

 No comments



Matthew Thompson (Courtesy of Raleigh City Council Bureau of Identification)

A Facebook photo leads to the arrest of a car theft suspect.

Cary Police charged Matthew Adam Thompson with burglary, possession of stolen goods, and breaking and entering after authorities were able to identify Thompson posing with a Mercedes Benz linked to a burglary in a Facebook photo, according to reports.

Thompson posed with his friend, Samuel James Clayton Harvey, who faces 10 charges of larceny and breaking and entering, according to WRAL. The photo in question had Thompson and Harvey posing with a reportedly stolen Mercedes in the parking lot of the apartment complex where Thompson lives.

Before the arrests, Cary Police said they had compiled evidence against Thompson and

<http://charlotte.cbslocal.com/2011/09/29/n-c-mans-facebook-photo-leads-to-arrest/>

Woman Violates Order Of Protection With Facebook 'Poke'

◀ 2 of 20 ▶



Police arrested Hendersonville, TN resident Shannon D. Jackson for allegedly violating the terms of an order of protection against her. Under the terms of the order, Jackson was forbidden from making contact with a certain Hendersonville woman, who claims Jackson defied the order by "poking" her on Facebook.

http://www.huffingtonpost.com/2010/08/16/arrested-over-facebook-po_n_683160.htm

Couple Arrested After Eating Rare Iguana On Facebook

◀ 6 of 20 ▶



Bahamian authorities apprehended an American couple over a series of Facebook photos detailing the capture, cooking, and consumption of a rare iguana. [Metro.co.uk](http://metro.co.uk) reported that the photos showed the couple "catching an iguana, parts of an iguana on a grill, two men eating the iguana pieces, and a man and a woman cleaning what appears to be undersized conch." Police tracked the couple down and arrested them for violating the Convention on International Trade in Endangered Species of Wild Fauna and Flora.

http://www.huffingtonpost.com/2010/08/16/arrested-over-facebook-po_n_683160.htm

Facebook your country's security away...

- ▶ Farce of the Facebook spy: MI6 chief faces probe after wife exposes their life on Net
- ▶ “ MI6 faced calls for an inquiry last night after an extraordinary lapse of judgment led to the new head of MI6's personal details being plastered over Facebook.
- ▶ Millions of people could have gained access to compromising photographs of Sir John Sawers and his family on the social networking website. ...“

<http://www.dailymail.co.uk/news/article-1197757/New-MI6-chief-faces-probe-wife-exposes-life-Facebook.html>



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>

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

41% of Facebook users willing to divulge info to Strangers

In an experiment, 41% of Facebook users were willing to divulge highly personal information to a complete stranger. This [according to IT security firm Sophos](#), which invited 200 randomly selected Facebookers to befriend [a bogus Facebook user named “Freddi Staur”](#) (an anagram of “ID Fraudster”). Of those queried, 87 responded to the invitation, among them 82 people whose profiles included personal information such as their email address, date of birth, address or phone number. In total:

- ▶ 72% of respondents divulged one or more email address
- ▶ 84% listed their full date of birth
- ▶ 87% provided details about their education or workplace
- ▶ 78% listed their current address or location
- ▶ 23% listed their current phone number
- ▶ 26% provided their instant-messaging screen name

Yikes. You’d think [institutional privacy concerns](#) would be enough to make folks think twice about expanding their Facebook networks with reckless gusto, wouldn’t you? Guess not.

<http://digitaldaily.allthingsd.com/20070814/facebook-privacy/>

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.

Threats: Governments & Corporations



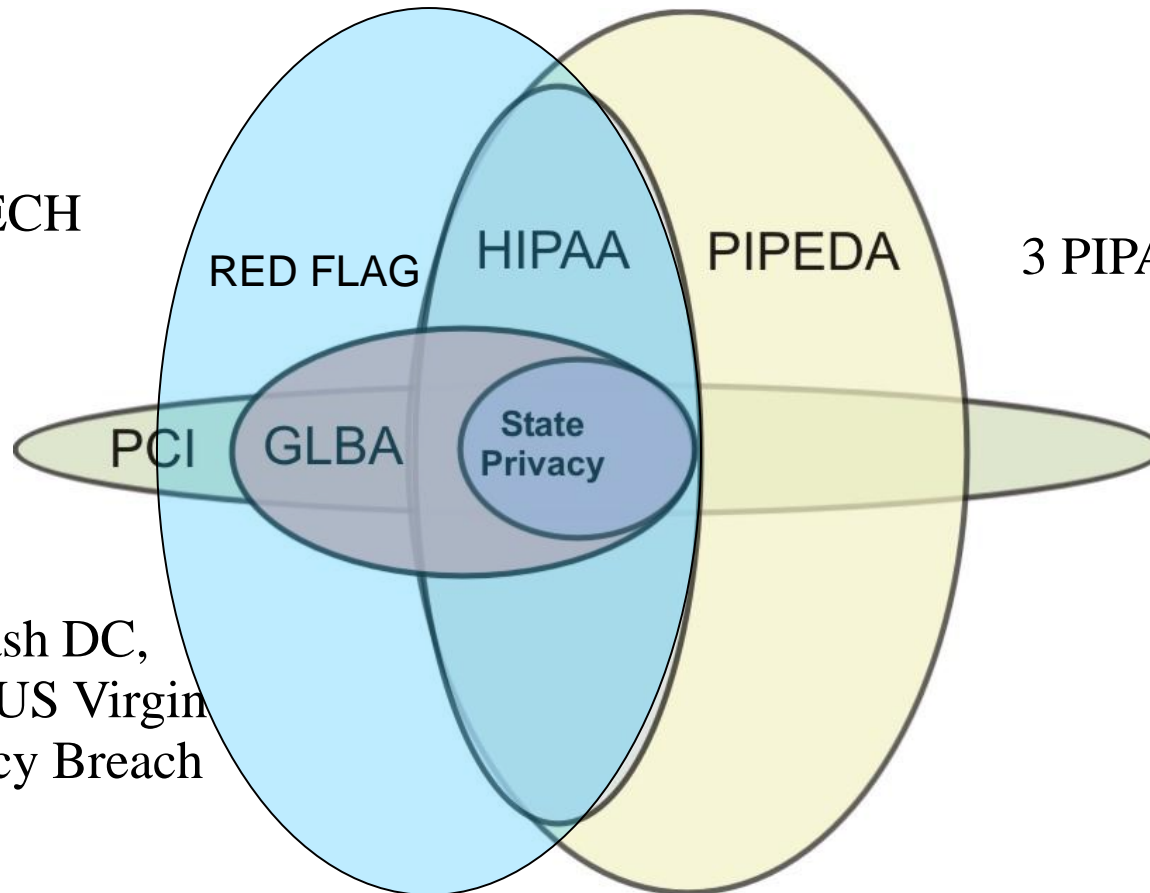
“Everything You Say Can And Will Be Used Against You, By Anybody, Now Or Decades Into The Future.” – Falkvinge on Infopolicy

Canada vs. US

US

HIPAA/HITECH
GLBA
RED FLAG

47 States, Wash DC,
Puerto Rico, US Virgin
Islands Privacy Breach
Laws



Canada

PIPEDA

3 PIPA/PPIPS laws

C-30 Canadian Spying Bill requires ISPs to log all traffic, give cops unfettered access

Terry Milewski writes on the CBC, the bill also gives the government the power to appoint special inspectors who can monitor and copy *all* information that passes through an ISP, also without a warrant. The inspector, says the bill, may "examine any document, information or thing found in the place and open or cause to be opened any container or other thing." He or she may also "use, or cause to be used, any computer system in the place to search and examine any information contained in or available to the system."

You read that right. The inspector gets to see "any" information that's in or "available to the system." Yours, mine, and everyone else's emails, phone calls, web surfing, shopping, you name it. In short, there's nothing the inspector cannot see or copy. "Any" information is up for grabs. And you thought the new airport body scanners were intrusive?

<http://boingboing.net/2012/02/17/canadas-spying-bill-also-all.html>

Canadian Public Safety Minister unaware of what's in his bill

Public Safety Minister Vic Toews says he is surprised to learn that a section of the government's online surveillance bill provides for "exceptional circumstances" under which "any police officer" can request customer information from a telecommunications service provider.

<http://www.cbc.ca/news/canada/story/2012/02/18/pol-thehouse-vic-toews.html>

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 youth 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 to 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 from 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 Indian 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.

It is encrypted email and BBM messages in particular that Indian cops are interested in, the Indian 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 Indian government, ending a stand-off that has lasted several years.

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/>

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

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

You 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

US operator Verizon Wireless is to log, and sell, customers' browsing and location history, unless 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.

The screenshot shows a Verizon Wireless privacy policy update. A large white callout bubble with a black border is centered over the text, containing the message: "You will receive mobile ads whether you participate or not, but under the advertising program, ads may be more relevant to you." Below the bubble, there is a section titled "Your choices" with two options: "If you do not want us to use your information for any of the purposes described above, please let us know at any time by" and "You will receive mobile ads whether you participate or not under the advertising program, ads may be more relevant to you." The background of the screenshot shows a table with columns for "HOW INFORMATION WILL BE USED", "DESCRIPTION", and "EXAMPLE".

HOW INFORMATION WILL BE USED	DESCRIPTION	EXAMPLE
To create business and marketing reports.	We will combine location change information and other data.	A report might state that 10,000 mobile users visited a sports website in a month and purchased a shirt.

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 to 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/

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/>

How much does Facebook Know about you? 800 pages worth

- ▶ In the EU, the citizens own their data. In the US, the corporations own the data.
- ▶ If you ask Facebook profile data in the US, you'll get laughed at.
- ▶ If you live in the EU however, you can request a copy of your profile data and Facebook is legally obligated to send it to you. www.Europe-v-Facebook.org is documenting the data that Facebook is releasing to EU users – from 192 pages to 800 pages PER person.
- ▶ From E-V-F: Every person in the EU has the right to access all the data that a company is holding about him/her. You can find out how to access your facebook data on the page “your data...”. After we got the first response by facebook it was clear to us that we had to publish this information online. By doing so, we want to make facebook more transparent and show every user which data facebook is holding about us.
- ▶ There is more Data. Many groups of data are not included in this first set of data we got from facebook. For example data concerning the “like”-function, tracking on other webpages, face recognition, videos, postings on other users walls, indicators for the intensity of relationships, tags that were removed and many more were so far not disclosed by facebook.via europe-v-facebook.org.

What Facebook knows about you is a **TRADE SECRET** and cannot be revealed

- In its terms, Facebook says that it does not guarantee any level of data security.
- Applications of “friends” can access data of the user. There is no guarantee that these applications are following European privacy standards.
- All removed friends are stored by Facebook. This was reconfirmed recently.
- Facebook is hosting enormous amounts of personal data and it is processing all data for its own purposes. It seems Facebook is a prime example of illegal “excessive processing”.
- Facebook is running an opt-out system instead of an opt-in system, which is required by European law.
- The Like Button is creating extended user data that can be used to track users all over the internet. There is no legitimate purpose for the creation of the data. Users have not consented to the use.
- via [Facebook: Releasing your personal data reveals our trade secrets | ZDNet](#).

Mark Zuckerberg's private Facebook photos revealed: Security 'glitch' allows web expert to access billionaire's personal pictures

- Facebook user reportedly exploited security loophole to access pictures
- Some images of Facebook CEO at home with girlfriend have never been seen
- He is pictured with Priscilla Chan at their \$7million house in Palo Alto

By MARK DUELL

Last updated at 10:14 AM on 7th December 2011

Comments (144) | Share | 38 | Tweet | 529 | Like | 3k

A series of photos from Mark Zuckerberg's private Facebook page were made public today after a web expert managed to gain access thanks to a glitch in the social networking site.

The bug in the website's photo reporting tool - which Facebook says was only temporary and has now been fixed - meant that users could access others' pictures even if they were private.

Users were able to look at the private photos by 'reporting' a profile picture as 'inappropriate', which then saw other photos displayed, such as those of Facebook CEO Mr Zuckerberg.



Private photos: Mark Zuckerberg holds up plates of chicken he appears to have just killed then fried himself

<http://www.dailymail.co.uk/news/article-2070749/Facebook-security-glitch-reveals-Mark-Zuckerbergs-private-photos.html>

Group Arrested For Allegedly Creating A 'Slandorous' Facebook Page Targeting Lebanese President

◀ 4 of 20 ▶



Ahmad Shuman, Naim Hanna, Antoine Ramia and Shebel Qasab of Lebanon were arrested after they created a Facebook page criticizing Lebanese President Michel Sleiman. The country has strict rules against "libel, slander and defamation," the *Telegraph* reported after Shuman was taken into custody. Authorities say that the page, titled "We don't want a hypocrite as president," strayed outside the "norms" of free speech.

One of the page's posts read, "You're like a snake; all you do is from under the table." Another said, "You're not worth my foot," according to the *Telegraph*.

"[T]he content is pure slander and aimed at undermining the head of state," the

Moroccan Man Jailed For Creating Fake Profile

◀ 8 of 20 ▶



Fouad Mourtada, a resident of Morocco, created a Facebook profile identifying himself as Prince Moulay Rachid, the Moroccan King's younger brother. Mourtada was arrested and sentenced to three years in prison for "villainous practices" and "identity fraud," according to TechCrunch.

http://www.huffingtonpost.com/2010/08/16/arrested-over-facebook-po_n_683160.htm

Thailand jails U.S. man for insulting king

[19 Comments](#)[Have Your Say](#)[Email Story](#)[Send to a Friend](#)[Share This](#)[Tell Your Friends](#)[Tweet This](#)[Tweet This](#)[More](#)[Share It](#)

Joe Gordon, a Thai-born American, center, is escorted by correction officials at a criminal court in Bangkok, Thailand, Dec. 8, 2011. (AP)

(AP) BANGKOK - A court in Thailand sentenced a U.S. citizen to two and a half years in prison Thursday for defaming the country's royal family by translating excerpts of a locally banned biography of the king and posting them online.

http://www.cbsnews.com/8301-202_162-57339098/thailand-jails-u.s-man-for-insulting-king/

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>

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

By **GRAEME MCMILLAN** | @graemem | January 12, 2012 | 16

Like 369 Tweet 1,200 +1 9 Share 56



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.

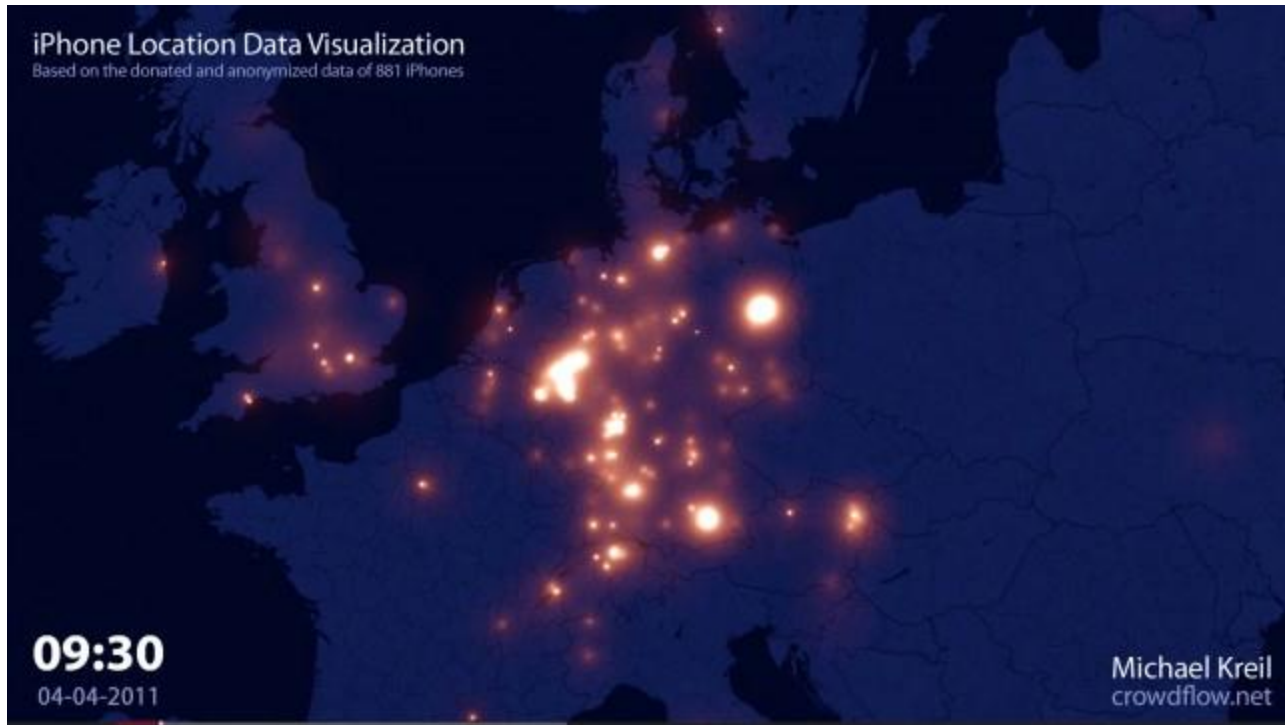
The "privacy compliance review" obtained by Reuters comes from last November, but apparently this surveillance has been ongoing since at least June 2010. According to the document, it's designed to "collect information used in providing situational awareness and establishing a common operating picture" 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/>

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/



A new visualization of cellphone location data surfaced [on Engadget](http://www.engadget.com/2011/07/16/crowdflow-tracks-880-iphones-across-europe-wants-to-put-you-on/) - <http://www.engadget.com/2011/07/16/crowdflow-tracks-880-iphones-across-europe-wants-to-put-you-on/>

Insight into the powers taken by European governments by means of the Data Retention Directive. Would you want the Police to be able to see your movements and the movements of all of your friends like this? Would you want the Police under any future government and set of laws to be able to track and correlate how you and your friends move, in real time and in recorded history, like this?

If the former East European governments had had this kind of visualization on their dissidents, they would still be around. The governments, that is, not necessarily the dissidents. - Falkvinge



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 Harbor 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 consulting 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>

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



NYIT Contact Information

Dr. Julia Saurazas, Ph. D.

Executive Director and Campus Dean

New York Institute of Technology

jsauraza@nyit.edu

604-639-0942