Supply Chain Operations & Technologies
Supply Chain Vendor Compliance
Fraud Detection & Reduction
Good Governance
Turnaround Help

Since January 1996

So the news broke out that the US government, specifically the National Security Agency (NSA), whose budget itself is classified as top-secret, is gleaning data from telecommunication carriers and Internet search providers, and folks are in an uproar.

If anyone caught the cover story of WIRED magazine's April 2012 issue, the NSA is building a massive data center in Utah that has the ability to store and analyze all telephone calls, e-mails, and Internet searches every one of us is doing, right down to analyzing the content. The proverbial cat was already out of the bag in a big way over one year ago. And per WIRED magazine's more recent July 2013 issue profiling General Keith Alexander, there's more big growth at the NSA to come.

Let's put the current news story in its proper perspective: in the interest of national security, the NSA is using pattern recognition to identify potential threats to our well-being. And this pattern recognition extends to not just the "from" and "to" points of the communication but also – apparently – it delves into some content analysis sometimes.

(The US Postal Service has been photographing the exterior of every piece of paper mail (letters and parcels) processed in the United States ever since the anthrax attacks in late 2001. The Mail Isolation Control and Tracking program records about 160 billion images per year, noting the from and to addresses, and has been used by other government law enforcement agencies such as the FBI, DEA, and Health and Human Services to track drug smugglers and Medicare fraudsters as well as those who send threatening letters to public officials.)

When it comes to the use of data and content pattern recognition, look no further then how social media giants such as Facebook® and LinkedIn® as well as search giant Google® determine who and what to present to us based on who and what we've liked and connected to or followed.

(I invite you to read Edward Wasserman's insightful editorial on Google Glass® in the June 10, 2013 edition of the Miami Herald newspaper for a deep-dive on how invasive this technology might just be going.)

Our retail purchase information is sold by merchants to mass data analyzers who figure that if we have the disposable income to buy quality meats through the mail, we probably have enough money to purchase high-priced watches, artwork, or apparel, and who then place a value on our identities and characteristics and sell our contact information for marketing use.

Truly the most "insidious" entity who knows a whole lot about me is my local grocery store. From my purchase history they know my shopping pattern (what day of the week and time of the day I am usually there), and could ascertain my family size, gender, health habits, dietary restrictions, lifestyle, and other attributes about me from analyzing my purchases. I use a credit card so my identity is known to my grocery store chain – I could only escape this truly if I paid with cash but I like getting credit card points and I don't like carrying all that cash around aside from the hassle of doing so, not that my bank might not leap to some conclusions based on a pattern analysis of my cash withdrawals either. Use of a loyalty card attaches my purchases to my personally identifiable information even easier.

In a truly egregious case of a retailer "listening" to the data it was collecting, a mass merchant, upon analyzing the items purchased from its customers' sales receipts, began sending targeted health and product bulletins (a.k.a. marketing material) to select consumers. These mailings were how the father of a teenager discovered his daughter was pregnant: the retailer's data mining ascertained the consumer was a female and likely pregnant based on the items being purchased. Was this an invasion of the teenager's privacy? What if she was not pregnant, e.g.

0 95494 24141 1

Visit our web sites:

http://www.katzscan.com/

http://www.supplychainfraud.com/

http://www.vendorcompliance.info/

http://www.turnaroundhelp.com/

http://www.supplychainsox.com/

Do you know of a company - *maybe your own* - suffering from disconnected dots?

www.disconnecteddots.com

Let's link!

www.linkedin.com/in/katzscan

Follow Katzscan on Twitter!

http://twitter.com/katzscan

Katzscan is on Facebook!

http://www.facebook.com/katzscan

purchasing the items for a friend in secret or a family member as part of the routine shopping? Should there not be laws against this kind of snooping and this kind of invasion into the lives of consumers? Where is the outrage here?

I probably have more to worry about from the merchants where I shop than my government because there are more legal restrictions placed on what the government can and cannot do versus what the private sector can and cannot do with the data they collect.

Concern over the NSA's data mining involves where the data is being stored, and my guess is right here in the US probably in that massive data center in Utah. However, who knows where retailers and marketing analytics companies are storing and sending our consumer data across the globe? Again, there are more legal and oversight protections in place at the federal government level than there are in the private sector.

Where is the outrage when millions of email addresses and passwords get hacked in the private sector? The result is that this seemingly disparate data is pieced together by smart criminals who utilize it for phishing scams and identity theft frauds, scoring significant amounts of money and consuming lots of law enforcement resources because there are ties to organized crime. And who pays for these law enforcement resources? Taxpayers like you and me.

Solid fraud detection and reduction relies upon data analysis and pattern recognition. If the Internal Revenue Service and Medicare both utilized better data analysis, fewer false tax returns where identity theft occurred would have been accepted and money disbursed, and fewer false medical claims/bills would have been paid. These frauds – especially Medicare frauds – account for billions of dollars per year in wasted taxpayer money.

So before we go overboard, let's think for a moment: there is nothing I personally put in an e-mail or say in a phone call that the NSA is going to find remotely of interest with regards to national security, let alone daily life. And putting this in perspective the chances of me being singled out by the government are likely much less than my being targeted by merchants for e-mail and postal mail advertising. We live in a very different – and dangerous – world today that utilizes telecommunications like never before. The private sector is listening in just as much (if not more) as the government and yet we are somehow all okay with this (even culpable in responsibility) despite the invasiveness, lack of security, and inaccuracies that abound. As I have nothing to worry about, and as an advocate of fraud detection and reduction, I say better safe than sorry, and I actually trust the government on this one.

Thank you.

Norman Katz, CFE, CFS, MOS
Katzscan Inc.

Look for the book --> http://www.gowerpublishing.com/isbn/9781409407324