Hal Berghel

MAKING PRIVATE RECORD PUBLIC, DO WE NEED TO GIVE OUT ALL OUR INFO?

In my last column, I discussed some of the current statistics on the extent of identity theft and financial fraud in the United States. You may recall that according to mainstream media reports, data security breaches account for the leaks of over four million individual, personal records, with cherished institutions like universities, local, state, and federal governments, and medical providers accounting for most of the leaks!

So it would appear that estimates of personal record compromises affecting tens of millions of individuals are likely to be reliable; hundreds of millions would not be surprising. This number is not easily extrapolated into expected dollar amounts because there is no one-to-one correspondence between a compromised record and a specific loss for a variety of obvious reasons.

One of the more alarming facts to emerge from Figure 1 is the percentage of contribution by healthcare providers, educational institutions, and governments. These three sources collectively account for one half of the total compromises. If we can't trust our colleges, hospitals, and government agencies to protect our confidential information, who can we trust? A breakout by breach instances follows the same pattern with the exception that there appear to be fewer breaches in the retail arena, but the breaches tend to involve a larger than normal number of personal records. This accord with our intuition because of the number of financial card transactions processed by merchants.

However, when we shift the focus away from the organization type and toward the nature of the breach, a different picture emerges - the majority of individual records compromised resulted from some form of online hacking. Well, what are we to do about this?

The fact of the matter is that we've all been drawn into the web of this conspiracy to make private records public. This happens subtly: a physician asks us for a social security number, a manufacturer asks us for our contact information for warranty purposes; the DMV wants to put your home address on your driver's license. And the most egregious and dangerous of conspiracies of all: car dealers who request personal information when you buy a car. None of this information is necessary for the purposes intended. Specifically, with the exception of Medicare billing, there is absolutely no medical reason for a physician to know your social security number, your address, your phone number, your mother's maiden name, your email address, etc. Medical history, yes; social security number, definitely not. Physicians collect this information for billing and collection purposes, period. There is no law that I know of that allows a manufacturer to disallow a warranty claim because the consumer refused to complete and return a warranty card. Manufacturers collect this information for purposes of marketing and revenue; they sell this information to third parties. While a state government is entitled to know where you live, they are usually not entitled to force you to have your home address on the driver's license (the importance of this issue will become clear below). And a car dealer, per se, is entitled to nothing. They must record information deemed sufficient by the state or municipality to transfer title. Anything beyond that is highly suspect.

So why do we give this information out? Largely because of herd mentality. Everyone else does it, so why not? Well, the reason is that these millions of records that are leaked each year producing billions of dollars of crime involve, for the most part, information that we voluntarily provided. We ought to know better. Toward that end, I offer the present column.

What's it all about, Alfie?

The business of blabbing personal information about us to everyone who asks dates back to the Social Security Act of 1935. Well, not actually to the Act itself, but rather other agencies, institutions, businesses, industries, etc. abuse of same. The SSA provides a mechanism by means of which every covered employee in the U.S. may be assigned a social security number for the internal use of the SSA. In less than ten years the idea of having a number for everyone was so appealing that the Internal Revenue Service wanted access

One of the more alarming facts to emerge from Figure 1 is the percentage of contribution by healthcare providers, educational institutions, and governments. These three sources collectively account for one half of the total compromises.

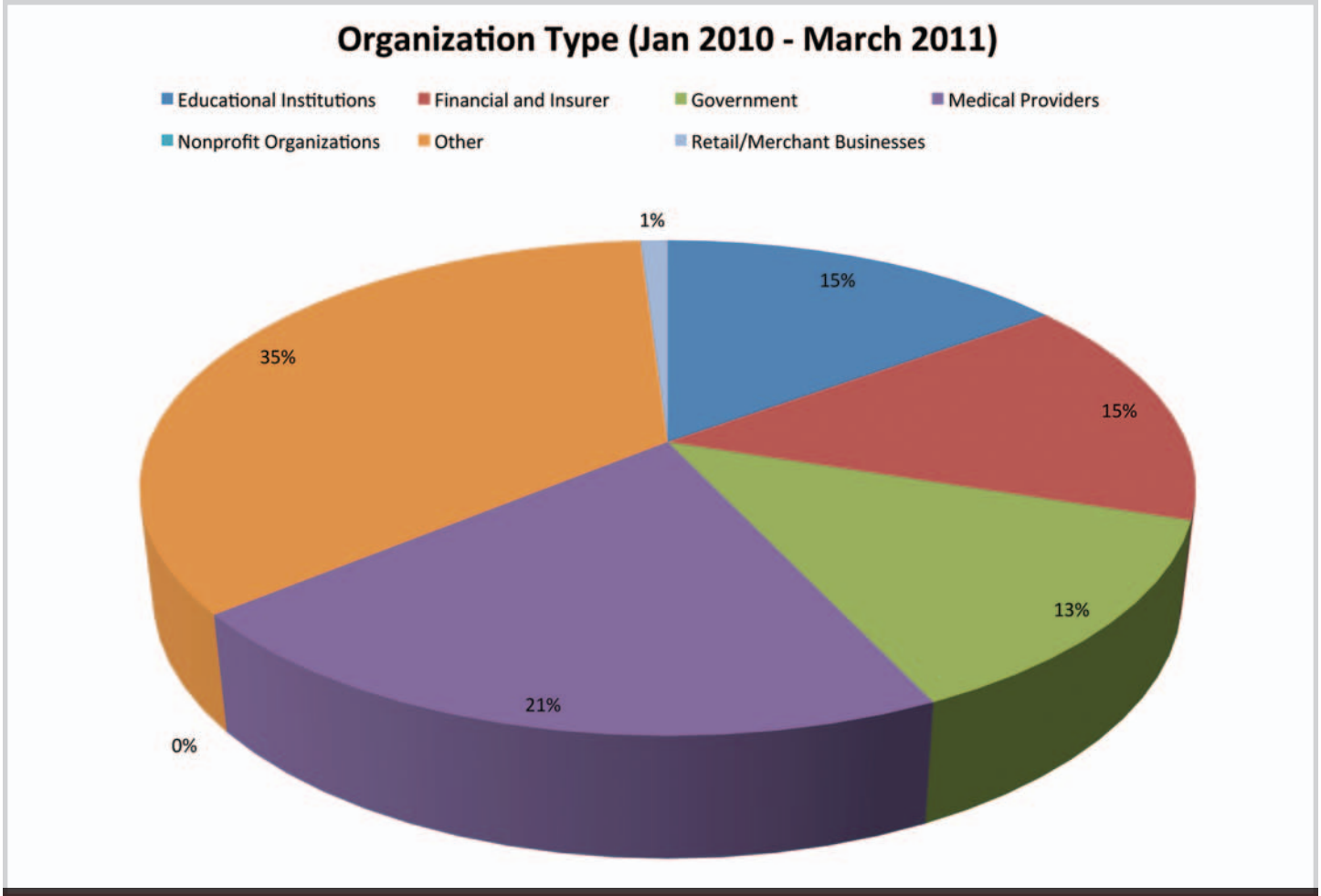

Figure 1: Distribution of Security Breaches of Confidential Personal Records by Organization Type (source: itffroc.org)

to it. And then other government agencies. Finally, in 1943, Executive Order 9397 extended the use of the SSN to all federal agencies. (I think you can see where this is headed). By the Federal Privacy Act of 1974, this got twisted into including state and local agencies, and we're off to the races. By this time every industry that dealt with the public felt entitled to know the SSN, and the toothpaste was completely out of the tube. For the past ten years, governments and agencies are trying to undue this stupidity with "Breach Notification Laws," that have met with some success. As of March 2009, forty four states and D.C. have passed such legislation. Alabama, Kentucky, Mississippi, Missouri (law is pending), New Mexico, and South Dakota notwithstanding. To their credit, some of the more progressive states (e.g., Michigan and Massachusetts) require that businesses that collect SSNs have information security programs that specifically address SSN protection. But most of the states with Breach Notification Laws limit their statutory prohibitions to such things as:

- publically posting, displaying or disclosing an individual's SSN;
- printing an individual's SSN on any card or tag required for the individual to access products or services;
- requiring an individual to transmit his or her SSN over the Internet without encryption or a secure connection;
- requiring an individual to use his or her SSN to access a website (unless a password is also required);
- printing an individual's SSN on any mailed materials; (vi) selling, leasing, trading or otherwise disclosing an SSN to a third party without consent of the individual; or
- encoding or embedding an SSN in a card or document in lieu of removing the SSN as required by law.

Of course the problem with such proscriptions is that the criminals don't follow the law! As a consequence, some advocates of personal privacy have advocated just eliminating the SSN and starting all over. No wonder. It's amazing how this seemingly harmless number has caused so many financial problems for the citizenry. This information can't be leaked if it's never collected.

The Worst Abusers

Without question the industry with the worst record in terms of protecting your privacy are the automobile dealerships. Where some manufacturers and physicians might try to coerce you into giving out personal information that they have no right to have, some automobile dealerships actually turn this into a blood sport. I'll give a few examples to illustrate this point.

The Old "OFAC" Scam: This happens when automobile dealers insist on personal information (e.g., SSN, bank information, complete contact

information) for cash purchases claiming that the federal Office of Foreign Assets Control (OFAC) requires it. OFAC "...administers and enforces economic sanctions programs primarily against countries and groups of individuals, such as terrorists and narcotics traffickers." Its charter is explained at http://www.treas.gov/offices/enforcement/ofac/faq/answer.shtml. The only way that you would be covered by OFAC would be if you were presumed to fall into one of the afore-mentioned categories. Customers have the right to insist on an explanation of why the dealership feels that they do. One frequently hears a mantra like "all purchases over $10,000 are scrutinized by the federal government. This is baloney. First, there is no mention of any $10,000 threshold, period. You can look this up yourself at http://law.justia.com/us/cfr/title31/31-3.1.1.1.2.5.1.1.html. Second, this law requires merchants to report transactions when they feel that the transactioner is likely a terrorist, criminal, narcotics trafficker, money launderer, etc. There is no presumption that every transaction by law abiding citizens be reported. If you confront this situation, ask the attendant sales manager to reproduce the legislation or statute that they claim defends their request. You'll wind up with no documentation because there isn't any.

The Old "Privacy Waiver" Scam: This happens when the dealership asks that you sign a privacy notice that waives your right to privacy. Why do they do this? Two reasons: (1) generate revenue, and (2) CYA. Dealerships may sell their customer's personal information to aftermarket add-on dealers (e.g., truck toppers, spoilers, sun shades, etc.). They may also use information about you for marketing purposes. They want you to sign the privacy notice so that they're not liable for any downstream inconvenience you might experience. NOTE: these privacy waiver forms are routinely sold to dealerships to increase their profits (see, e.g., Reynolds and Reynolds Law Form No 750S-PNNA which is commonly used in my area). Let me quote from this form so that you get an idea of what I'm talking about:

Without question the industry with the worst record in terms of protecting your privacy are the automobile dealerships. Where some manufacturers and physicians might try to coerce you into giving out personal information that they have no right to have, some automobile dealerships actually turn this into a blood sport.

Collection of Private Information we may collect the following kinds of Private Information about you from the following sources:

- Information you provide on applications, forms, or other correspondence, such as your name, address, social security number, and income.
- Information about your transactions with us or others, such as your account balance and payment history
- Information we receive from consumer reporting agencies, credit references, employers, insurance companies, and insurance agencies, such as your credit history and credit worthiness, and information that we obtain to verify employment history or that insurance coverage is in force.

Disclosure of Private Information - We may disclose some or all of the Private Information (described above) under the following circumstances:

- To marketing service providers and joint marketing partners - We may disclose Private Information to companies that perform marketing services for us or to other financial institutions with which we have joint marketing agreements.
- With non-affiliated third parties - We may disclose Private Information about you with non-affiliated third parties permitted by law."

The intent of the form is pretty clear from the wording. This is not in the customer's interest, period! There is no reasonable consumer-centric justification for this. And what makes matters worse is the cavalier way in which dealerships handle this information. I was once told by a dealer that all information would be photocopied and then destroyed after entry into their ultra-secure database. Those of you who follow these columns know about the insecurity with photocopiers.

So What's a Person To Do?

Well, I've got a remedy for you to consider. But first a few caveats. First, if you follow my advice you may have to change doctors, insurance agencies, car dealerships, etc. But if you've already dealt with them, the battle is already lost so if you follow my advice, there will be no harm, no foul. Second, I'm not an attorney, so these recommendations are offered from

The business of blabbing personal information about us to everyone who asks dates back to the Social Security Act of 1935. Well, not actually to the Act itself, but rather other agencies, institutions, businesses, industries, etc. abuse of same.

AVATIER™

The newest luxury resort casino & hotel on the Las Vegas Strip...

4,400 New Hires in 4 weeks

Avatier, the next-generation Identity Management solution provides blazing fast deployment of your User Provisioning, Password Management and Identity Governance system. Your dollars are spent on configuration not development. Gone are the days of complex programming, Avatier uses its patented IT shopping cart to empower IT and business operations, to easily welcome and exit your employees.

10 YEAR G&L GAMING & LEISURE ANNIVERSARY

GAMING & LEISURE
BUSINESS PARTNER

Demo the future of Identity Management, call 1-800-609-8610 or sales@avatier.com • www.avatier.com

one technologist to another. My recommendations are no substitute for professional legal advice.

So, here we go. The following the generic advice harvested from FTC, FBI, BBB, etc websites:

- shred
- protect SSN - don't give out unnecessarily
- don't use revealing data as userIDs/pswds (e.g. MMN, last 4 of SSN)
- keep personal data in safe place
- monitor financial/billing accounts
- pay attention to arrival dates
- beware unauthorized CCs or accounts
- investigate surprising credit denial
- get free annual credit reports from Experian, transUnion, Equifax
- close unused accounts
- keep PIN numbers hidden

So far, so good. However, this list has been "sanitized" to be merchant and vendor friendly. As such it is really incomplete as it stands. To be really effective in the protection of personal privacy, one needs to be more aggressive. Toward that end, I offer the following advice for your consideration:

- DO NOT give out SSN to any non-gov't agency unless required to do so by law, and ask to see a copy of the law. This includes banks, health-care providers, car dealers, loan companies, even employers except those legally obligated to report wage information to government agencies.
- DO NOT use your SSN on any form of identification, including
  - DMV IDs including Driver's Licenses
  - Work Permits
  - Insurance Cards
  - Employment IDs/Badges
- DO NOT have any personal contact information on your person unless required by law (the criminal may get your wallet, but they won't where to find you). Use a post office box for all identification whenever allowed by law. Specifically, use P.O. Boxes for driver's licenses (and DO NOT allow SSN nor reversible hash of same to be used) vehicle/boat registrations
- Insist that authorized personal data on websites (email address, office info) be MUNGED to prevent harvesting, this especially applies to employers
- Insist that unauthorized personal data on websites be removed. Responsible webmasters will respect "takedown" notices

- DO NOT give out contact information to vendors and merchants. Car dealers, cell phone companies, pharmacies, and even physicians do not need to know your land line phone number and street address.
- DO NOT have your home address on the GPS in your vehicle. To be even more secure, consider password protecting your GPS.

THINK before buying any automobile with built in monitoring and tracking capability. These systems are controlled by the manufacturer and may be turned on or off with neither your knowledge nor permission. This came to light during recent court cases which revealed that law enforcement used them to "wiretap" conversations in vehicles. In fact, in 2011 GM's OnStar extended their EULA to cover their right to collect and sell personal information about the owner's vehicle, location, etc. to third parties. Note in the OnStar press release, below, that when the owner cancels OnStar, the default is that the connection remains active and continuously monitored by OnStar.

> *"Under our new Terms and Conditions, when a customer cancels service, we have informed customers that OnStar will maintain a two-way connection to their vehicle unless they ask us not to do so. In the future, this connection may provide us with the capability to alert vehicle occupants about severe weather conditions such as tornado warnings or mandatory evacuations. Another benefit for keeping this connection "open" could be to provide vehicle owners with any updated warranty data or recall issues.*

There is no legal obligation on OnStar's part to permanently disable the system; you have to take their word for it. If you want to be sure, don't buy a car with such systems, or have it disabled by a reliable technician.

- DO NOT let anyone photocopy personal documents if you can possibly avoid it
- DO NOT use an outside mailbox for important communications, use a P.O. Box instead. (Just the cover of mail betrays a lot of information about you, your financial situation, your employment, your known associates, etc., - information which you don't want criminals to have. "Mail Cover" is such a powerful investigative technique that its use is carefully regulated by U.S. Postal Regulations (39 C.F.R., sect 233.3).
- DO NOT de-commission photocopiers without first scrubbing or destroying the hard disk.

And finally, DO NOT look for any silver bullets when it comes to protecting your identity - there are none. The only defense is eternal vigilance.

Hal Berghel is Director of both the UNLV School of Informatics and the Identity Theft and Financial Fraud Research and Operations Center (itffroc.org). His consultancy, Berghel.Net, provides security and management services to government and industry.