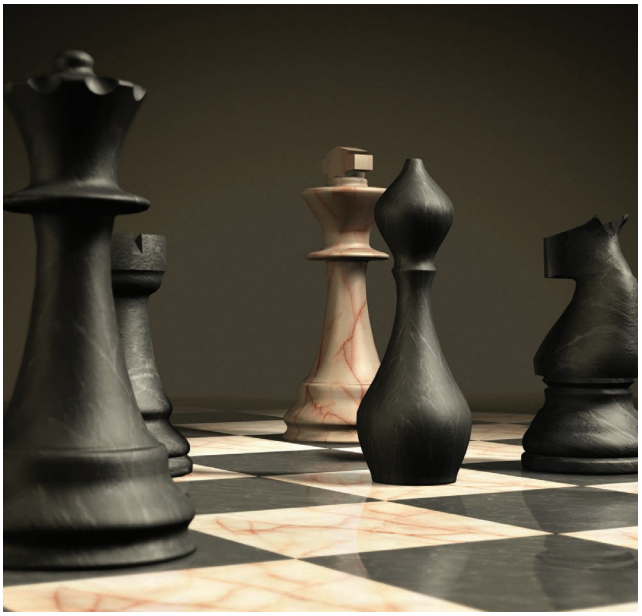

PII, the FTC, Car Dealers, and You

Hal Berghel, *University of Nevada, Las Vegas*

Personally identifiable information (PII) is among the most digitally delicate data and deserves maximum government protection. So why isn't it better protected? Here are some thoughts on the matter.

Science fiction writer Robert Heinlein is said to have remarked that privacy laws only make the spy-bugs smaller. This remark abounds in pith. At a practical level, the cornucopia of surveillance gadgetry confirms its validity. But most of all, this observation belies the painful truth that there's really no end to the potential abuses to personal privacy by corporations, criminals, and governments.

The most sensitive information about us is our personally identifiable information, or PII. While there are many definitions and contexts from which PII might arise, consider it to be information that can be used, either independently or collectively, to identify, contact, or locate a unique individual.[1] I'll discuss some historical causes of PII vulnerability and suggest some tactics for minimizing your PII footprint.

THE FTC AND MISSION SLIP

We live in a world where good ideas get so corrupted by politicians that it's often hard to recognize the original intent from the result. Such is the case with the National Do Not Call Registry, which was specifically drafted with loopholes to allow political robocalls, not-for-profit solicitations, unsolicited contact by surveyors and pollsters, and "follow-up calls"—all to benefit special interests. The goal of protecting the public communications infrastructure from unwanted, bothersome nuisance communications somehow got lost in the congressional debate. This process of accommodating political interests at the expense of the public is now so widespread that it's laughable. The CAN-SPAM Act has come to be known as the "You-Can-Spam Act" in some circles, just as the Junk Fax Prevention Act is called the "Junk Fax Protection Act." Incidentally, these three federal statutes have two things in common: they were products of the George W. Bush presidency, and they never worked as envisioned.

In plain terms, these statutes were a product of a dysfunctional Congress and a Federal Trade Commission (FTC) that lost much of its consumer and citizen advocacy stamina over the past 30 years of frenzied deregulation. Even the well-intentioned FTC has been hamstrung by the business lobbies, antiregulation forces who cast consumer protection as regulatory overreach, and a leadership selection process that is inherently partisan.

Like many of you, I've developed a daily routine around separating myself from unwanted faxes, email, text messages, and telemarketing—all of which are explicitly illegal under these federal statutes, and all of which could be trivially prevented

Published by the IEEE Computer Society
0018-9162/14/$31.00 © 2014 IEEE

with current technology and a proactive government. And yet, like the Nigerian 419 scam, the intrusions into our privacy won't go away.

I don't blame the FTC. It's between a regulatory rock and a pro-business hard place. Despite its worthy aspirations, the FTC lacks both the manpower and political independence to remain effective beyond the periphery of its mission. I call this "mission slip." Notable FTC accomplishments, like suing LifeLock for false advertising[2] or security company ADT for failing to disclose that its "expert witnesses" were paid endorsers,[3] tend toward the inconsequential and are noteworthy for the minimal penalties levied against organizations and corporations that can't bite back. Don't expect aggressive prosecution of multibillion-dollar multilevel marketers, too-large-to-regulate financial institutions, stakeholder media interests, or energy or communication oligopolies with a strong base of support and endless legal resources. The Sherman and Clayton Antitrust Acts won't be able to rely much on the FTC: trust-busting is no longer in the FTC's vocabulary! The FTC has done little of late to impede the concentration of ownership in industries, from healthcare to food processing to the financial sector to big pharma to big oil. You can see why that's so in the FTC's most recent mergers and acquisitions guidelines.[4]

You can derive some sense of how the FTC rolls these days from a 24 September 2013 speech by one of the Republican Commissioners.[5] Note that the recent antitrust successes he mentioned were *Federal Trade Commission v. Phobe Putney Health Systems, Inc.*, which challenged a Georgia immunity doctrine for a small hospital authority, and *Federal Trade Commission v. Actavis*, which challenged a "reverse payment" settlement between small-brand and generic pharmaceutical companies. The healthcare industry and big pharma won't quiver over the FTC's ruling in these cases. So, look for the future FTC to weigh in on matters relating to teeth whitening, nutrition, and the most outrageous deceptive advertising.

BLACK BOXES, ORANGE BOXES, AND CAP'N CRUNCH REVISITED

As an aside, our statutes actually created a cottage industry for lame technologies such as caller ID and the special information tone (SIT) generators that used in-band technology to detect and circumvent telemarketing. These technologies were as ineffective as the statutes they sought to reinforce. Caller ID was rendered largely ineffective by caller ID spoofing (which, incidentally, remains in use in the current IRS phone scam[6]), and SIT generators were simply ignored by next-gen predictive dialers. Now that the telcos have moved to the newer, packet-based SS6 and SS7 protocol suites, the criminals can be counted on to use modern packet-based hacking tools. Telco attempts to use simple technological tricks to thwart telephony scams will never succeed. As they did in the 1960s and '70s, criminals will always find a new, son-of-blue-box, orange box, or Cap'n Crunch whistle to circumvent telco technology. For a good overview of modern digital telephony and the next wave of vulnerabilities introduced therewith, see "SCTPscan—Finding Entry Points to SS7 Networks and Telecommunication Backbones,"[7] by Philippe Langlois (and www.youtube.com/watch?v=yK19yXYlFOY).

By closing the statutory loopholes demanded by the business lobbies and written into the statutes by a beholden Congress, adding in some consumer-friendly telco refinements, and following up with a few rounds of aggressive enforcement, this game of technology leapfrog could be avoided. On the telco side, personalized call-blocking by individual source at the handset would be a great start. Complimentary subscription call-blocking blacklists would serve modern telephony just as spam and Web blacklists serve email and Internet users. These tools have thus far not been implemented, but not because they're too expensive or complicated, rather, because such things would incur the wrath of special interests.

This process of accommodating political interests at the expense of the public is now so widespread that it's laughable.

JUST SAY NO!

So that's the legislative backdrop against which our PII's vulnerability must be placed. As a consequence of the feckless legislation and uncooperative telcos, safeguarding is pretty much left to consumers and end users.

As a starting point, there are online federal[8] and non-government organization[9] resources, but they tend to make fairly obvious and ineffectual recommendations. A better online source is Robert Ellis Smith's *Privacy Journal*[10]—a resource that I recommend without reservation. In addition, I offer the following modest embellishments.

When your Social Security number is requested, get in the habit of saying "no." Don't give it out, period. Your physician, health insurance company, landlord, lawyer, and car dealer have no compelling

legal reason to even ask for it—or your mother's maiden name, place of birth, or sexual history, for that matter—unless you specifically agree to a search of your credit history. Federal law only requires the use of Social Security numbers by selected federal agencies like the Social Security Administration, the Internal Revenue Service, and Medicare. That said, if your doctor refuses to serve you without it (doctors build as complete a profile on you as they can to ensure payment), find another one.

But let's go one step further. For your own protection, don't carry your Social Security number (especially not your card) on your person unless you're legally required to present it. Social Security cards belong in safe storage with your other important papers. Those who need the number either already have access to it or can confirm it through the SSA directly, if so authorized.

And while we're at it, don't have anything on your extended person (including mobile devices, cars, offices, and lockers) that has your physical address on it. If criminals separate you from personal property, and like what they get, don't incentivize them to return for more. Progressive states have allowed the use of post office box addresses on auto registrations, driver's licenses, and IDs for many years. The last time I looked into this, only a few states were holdouts. You can find out your state's policy by calling local law enforcement. Follow this theme, so that criminals can't use your possessions to find you. And it goes without saying that mobile devices should have minimal contact information out of respect for the PII of your contacts.

I continue to be surprised how many people have entered their home address for "home" on their GPS. A better idea is to use a convenient building or cross street a few miles from your home to return-navigate on long trips. If you can't find your way home from the nearest post office or shopping mall, you might want to consider a designated driver.

The Sherman and Clayton Antitrust Acts won't be able to rely much on the FTC: trust-busting is no longer in the FTC's vocabulary!

Needless to say, your contact information in public registries, such as telephone books and online directories, should refer to post office boxes and, whenever possible, answering services or machines. I also recommend using email aliases or forwarding services for all public disclosures of your email address together with a munge of your email address to make it more difficult to harvest from online directories with screen-scraping software. The munge doesn't have to be terribly fancy—throw in random spaces, corrupt the spelling of "at", use "period" or "dot" instead of periods, and so on. "h lb –a*t*--com pu ter—dot --org" works fine for me. Screen scrapers harvest the lowest-hanging fruit; they typically don't employ computationally expensive parsers to reconstruct email addresses from munge. They get enough email addresses using simple algorithms.

Use the onion routing service, TOR, for Web access whenever possible and track the status of anonymizing email services. The more popular email anonymizers (TorMail, Silent Mail, and Lavabit) closed in late 2013, after the FBI issued a spate of national security letters forcing ISPs and email service providers to reveal the contact information of their users. If and when these services return, they're worthy of your consideration. I'll have more to say about this in a future column.

Finally, for all printed media that has your contact information on it, use a manual "cross tear." For junk mail, tear the entire envelope through the address field, put the smaller part in the trash and the larger part in the recycle bin—it's the green thing to do. And don't carry a debit card on your person. If you're into plastic, use credit cards that provide more complete fraud protection capability.

CAR DEALERS AS WEAPONS OF MASS INTRUSION

Finally, one of the most offensive and brutish intrusions into the PII space comes from car dealers. Always a handy source for brutish and rude behavior, car dealers in the digital age can deploy weapons of mass intrusion. It's not unusual for them to ask for information from you for which there is no legal justification, sell your private information to third parties, request that you take actions that are against your economic and legal interests, and—as if that's not enough—misrepresent their product and the laws that govern its sale. In the best of cases, we would all have an attorney present when we deal with car dealers. Failing that, my final suggestions might provide you with information that can at least make you aware of the important issues involved.

An automobile is considered "personal property" under the law. In fact, it's considered "tangible" personal property in the same class as your watch, your toaster, and your pet hamster—versus "intangible" personal property like stocks and bonds. Under the law, if you own property, you're entitled to control its use, benefit from it, sell it, and recover damages if someone

else uses or damages it without your permission. In most cases, the car's owner will have actual possession, meaning that he or she will maintain physical control over it. When a vehicle is bought and sold, the seller transfers a title or certificate of ownership to the buyer. However, the seller can't sell a better title than he or she has—in other words, the seller can only pass on the right, title, and interest that he or she has, which might be nil, so caveat emptor applies.

In the US, property rights are determined by the states. Issues such as who can own personal property, how different classes of personal property are distinguished, how personal property is taxed, how personal property is secured, how transactions are recorded, and so forth are resolved at the state level. This is important because automobile transactions are regulated by state law. In some cases, car dealers are "creative" with regard to their interpretation of the law, and may seek to impose this creativity on the unsuspecting consumer.

To give one such example, even if there are no requirements with respect to the legal age of ownership of personal property, some dealers claim that by law, the dealer must retain a copy of the driver's license from all co-owners whose names appear on the bill of sale. You might list your 14-year-old as a co-owner of a new car: Could a state reasonably expect that a 14-year-old has a driver's license? Perhaps the car dealer wants this information for its records, to derive income by selling it to third parties, or for some other reason it isn't disclosing to the buyer. Of course, it's possible the car dealer wants to assure itself that anyone who drives the vehicle away from its lot has a valid driver's license for liability reasons, but this a completely separate issue.

Here's another example. Some car dealers might require the customer to sign a privacy notice that waives the customer's rights to privacy or a loan application form—even for cash sales. There's no *legal* justification for this, and the car dealer has no legitimate reason to expect the customer to agree to it. Industry insiders have suggested to me that there are two main reasons for the use of this form: first, the dealership is under investigation or has been the subject of complaints regarding its business practices, and it requires this signed form so that customers can't later sue them for unauthorized use of personal information; and second, the dealership relies on the income from the sale of personal information to third parties. In either case, this works against the interest of the customer. I would

go so far as to recommend that you avoid doing business with any dealership that uses general privacy waivers like this. There are plenty of car dealers.

These observations are not intended as a substitute for appropriate legal counsel, but they may make you aware of typical abuses.

I first expressed my concerns about digital invasions of privacy in *Computer* in January 2001.[12] From then until now, things have gone from bad to worse. Unfortunately, when it comes to PII, all of the legal caveats (*emptor*, *venditor*, *lector*, *utilitor*, and so on) still apply. The only escape from merchant abuse is eternal vigilance.

References

1. E. McCallister, T. Grance, and K. Scarfone, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," *Recommendations of the National Institute of Standards and Technology,* special publication 800-122, NIST, Apr. 2010; http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.
2. "LifeLock Will Pay $12 Million to Settle Charges by the FTC and 35 States That Identity Theft Prevention and Data Security Claims Were False," press release, Federal Trade Commission, 9 Mar. 2010; www.ftc.gov/news-events/press-releases/2010/03/lifelock-will-pay-12-million-settle-charges-ftc-35-states.
3. K. Bachman, "FTC Busts ADT for Failing to Disclose Paid Endorsers: Spokepeople Posed as Independent Experts," *AdWeek*, 6 Mar. 2014; www.adweek.com/news/advertising-branding/ftc-busts-adt-failing-disclose-paid-endorsers-156146.
4. *Horizontal Merger Guidelines*, US Dept. of Justice and Federal Trade Commission, 19 Aug. 2010; www.ftc.gov/sites/default/files/attachments/merger-review/100819hmg.pdf.
5. J.D. Wright, "The FTC's Role in Shaping Antitrust Doctrine: Recent Successes and Future Targets," FTC Commissioner's remarks, 2013 Georgetown Global Antitrust Symposium Dinner, 24 Sept. 2013; www.ftc.gov/sites/default/files/documents/public_statements/ftc%E2%80%99s-role-shaping-antitrust-doctrine-recent-successes-and-future-targets/130924globalantitrustsymposium.pdf.
6. G. Wallace, "IRS Monitor: $1 Million Phone Scam 'Largest Ever,'" *CNNMoney*, 24 Mar. 2014; http://money.cnn.com/2014/03/20/pf/taxes/irs-phone-scam.
7. P. Langlois, "SCTPscan: Finding Entry Points to SS7 Networks and Telecommunication Backbones," Blackhat Briefings Europe, 2007; www.blackhat.com/presentations/bh-europe-07/Langlois/Presentation/bh-eu-07-langlois-ppt-apr19.pdf.
8. "How to Keep Your Personal Information Secure," FTC Consumer Information, July 2012; www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure.
9. "Secure Your ID Day," flyer, Better Business Bureau; www.bbb.org/us/storage/0/Shared%20Documents/secure%20your%20id%20day/everyday%20habits.pdf.
10. R.E. Smith, "Tips for Individuals and Organizations: A Guide for the Frugal Privacy Seeker," *Privacy J.*, Mar. 2014; www.privacyjournal.net/bio.htm.
11. "OFAC Frequently Asked Questions and Answers," US Dept. of Treasury, 10 Mar. 2014; www.treasury.gov/resource-center/faqs/Sanctions/Pages/answer.aspx.
12. H.L. Berghel, "Cyberprivacy in the New Millennium," *Computer,* Jan. 2001; pp. 132–134,

Hal Berghel, *Out of Band column editor, is an ACM and IEEE Fellow and a professor of computer science at the University of Nevada, Las Vegas. Contact him at hlb@computer.org.*