Privacy Informatics: A Primer on Defensive Tactics for a Society under Siege

Hal Berghel, *University of Nevada, Las Vegas*

What the world needs now is a new field of study: privacy informatics. This emerging field will fill the information-awareness gap between a trusting citizenry and the emerging digital dystopia.

How did we get here? With the current state of privacy abuse and our wholesale sellout to the surveillance society, it's clear that our elected representatives have become the lapdogs for business interests that derive benefit from eavesdropping economics. We enjoy the collateral benefits of the technologies used in security cameras for home protection, GPS for navigation, RFID cards for everything from access control to vehicle telematics to cardiac pacemakers, OnStar for emergencies, the Web for ecommerce, and so on. Along the way, it never occurred to most of us that the technology that enables a call for help in an automobile accident could also be used to record personal meetings in a car, or that those recordings could be used to convict people of crimes. From a technology perspective, you can't have one without the other; it's a packaged deal.

We're also an increasingly distracted society. With television, radio, advertising, Web surfing, social networking, and texting, we have a potpourri of digital distractions. As media critic Neil Postman put it, we're "amusing ourselves to death," and that has led us to a Huxleyan (versus Orwellian) dystopia, where talking heads and visual images distract us from issues of genuine importance. In *Modernity and the Holocaust*, sociologist Zygmunt Bauman said that "rational people will quietly, meekly go into gas chambers if only you allow them to believe that they're bathrooms." In the same way, we digital denizens march willingly to a future where the price for privacy is digital death. We did this to ourselves, by behaving rationally and passively, because, as Bauman further noted, "the rationality of the ruled is always the weapon of the rulers." Today, the "rulers" are the political and financial neoliberal elite who have significant vested interests in their own information monopolies.

We bear this responsibility whenever we provide personal information to geneology and social networking sites, credit card companies, e-commerce businesses, healthcare professionals, schools, religious organizations, and so on. Of course, a minimal amount of information is required to sustain social interaction and commerce, but as a society, we maxed out on that generations ago. Everyone who uses the cloud, social networks, and smartphones without use of anonymization and encryption is part of the problem.

So, where do we go from here?

I offer here the poor person's substitute. It won't fix your privacy problems, but it's better than nothing.

BETTER-THAN-NOTHING PRIVACY DEFENSES

Ten years ago, I launched Better-than-Nothing-Security-Practices (http://www.berghel.net/btnsp/btnsp.php) in a desperate attempt to satisfy some basic security needs for clients and audiences. Nowhere near the depth, breadth, and quality of SANS training—which is the single most important resource for security training in the world (http://sans.org)—my approach to security had the distinct advantage of being free. I'm comfortable in speculating that it lived up to its name.

Ten years ago, I devoted attention to publicizing security threats from hackers and criminals. These days, I'm devoting my efforts to educating people about privacy threats from government and industry. Although the players' wardrobes and beverage choices have changed, the abuse of the electorate remained constant.

This is the first installment of my Better-than-Nothing Privacy Practices series. In this episode, I'll focus on two common tools: browsers and cell phones—specifically, Mozilla Firefox v24.0 and Android v2.3.3, two tools that I rely on heavily. My goal here is to raise the bar a little to discourage those digital demons who might wish to violate our privacy.

A decade has elapsed, and the world's digital concerns have shifted from mostly security to a balance between security and privacy. Edward Snowden's greatest contribution could be that he, more than any other individual, added fuel to the global debate on privacy.

FIREFOX AND THE ADD-ON WARS

From the version numbers, it's clear that I don't update my Android, but I do keep Firefox current. This is due to the very different levels of trust I have in the companies and products involved.

The initial configuration of Firefox is critical in preparing for add-on privacy enhancements that I'll return to in a few paragraphs. Just to set the stage, I'll offer a few observations for those who aren't in the habit of tweaking their browser security and privacy settings. For more thorough analyses, readers are directed to the wealth of online resources.

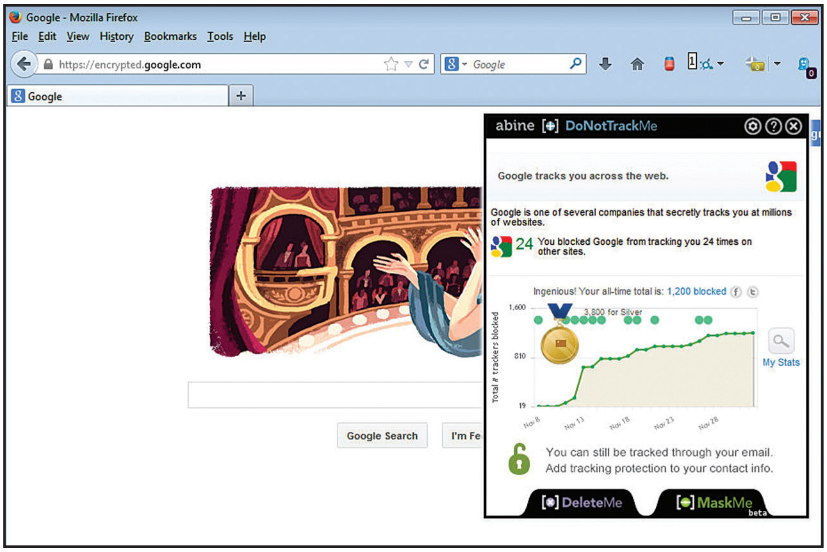
We begin with the Mozilla privacy panel (Menu bar>Options>Privacy Tab). I recommend, for your consideration, checking "Tell sites that I do not want to be tracked" (the so-called Do Not Track option). Under "Use custom settings for history," I recommend checking both "Always use private browsing mode" and "Accept cookies from sites." However, for "Accept third-party cookies," the preferred option is "Never." Set "When using the location bar, suggest" equal to "Nothing." Using the custom settings option in this way automatically clears the history when Firefox closes (a byproduct of private browsing mode). It's always wise to click on "Show Cookies" now and again to inspect for cookie crumbs. Actually, I occasionally force my browser to manually discard cookies and other cache items like scripts, such as <ga.js>, to minimize the risk of packet injection. A delightful little add-on, the Empty Cache Button, works well for this. It's amazing how hard it is to keep the net snoops' mitts off our cache.

Now let's see what we've accomplished. First, the Do Not Track option falls under the category of "gratuitous act of defiance for optimists" (see this column, September 2013). DNT is an accepted Internet Engineering Task Force (IETF) HTTP header field, but (and here's the rub), it's *not* a "core" header field and hence *not* required for IETF compliance. Simply put, servers and network appliances can ignore without penalty and remain in conformance with standards.

So, why do it? Because some web servers are respectful of the user's privacy, and so in those cases, DNT works. Many of us continue to call for rigid enforcement of DNT, and someday this might pay off. (I'm not holding my breath, since corporate America is the de facto regulator of the Internet.) In any case, after a reboot of Firefox, these settings should produce no recorded history and minimal cookie crumbs.

The History and Location Bar recommendations limit the amount of "browser guano" left on the computer. Firefox originally included history and location bar options to limit the recovery of this information from public or shared computers. However, in the age of warrantless wiretaps, extrajudicial detention, and penetration of journalist's shield laws, it's wise to consider how we might prevent this information from getting through in the first place. Any minimal inconvenience is more than offset by the increased protection against computer activity mining by government, law enforcement, private surveillance merchants, and corporate information harvesters. Needless to say, this will undercut the use of the Awesome Bar—Firefox's self-adapting browser bar.

The rationale for this sort of privacy configuration is that it minimizes exposure of access to user behavior by prying eyes, legal and not. I emphasize "minimize" here because browser developers are less than transparent these days on where they hide this stuff. Earlier versions of Firefox, for example, allowed the user to specify the location of the browser cache. That made monitoring and cleanup straightforward. Now, Firefox buries



Google tracks you across the web.

Google is one of several companies that secretly tracks you at millions of websites.

24 You blocked Google from tracking you 24 times on other sites.

Ingenious! Your all-time total is: 1,200 blocked

You can still be tracked through your email. Add tracking protection to your contact info.

Figure 1.Smooth running with NoScript can be completely transparent. In this case, all scripts have been disabled. The inset is the DoNotTrackMe report that runs concurrently.

sundry metadata and browser guano as history, bookmarks, cookies, configuration settings, passwords, autocomplete histories, and so on, in a special profile folder (on Windows computers, %APPDATA%\Mozilla\Firefox\Profiles), much in encoded or encrypted form, so there's no easy way to find and inspect it. Mozilla claims that having this profile isolated from the application is a feature, because the data integrity isn't dependent on the stability of Firefox. Baloney. This is just another developer's way of restricting user behavior for its own convenience and self-serving purposes. Making the eradication of browser guano a hassle for the user serves the interests of myopic software developers who believe that their vision of computer use trumps the privacy interests of the customer. For those interested in more detail, I've discussed the recovery of such residue under the rubric of BRAP (BRowser and APplications) Forensics elsewhere (www.berghel.net/col-edit/digital_village/jun-08/dv_6-08.pdf).

Now, on to the security settings (Security tab). Check "Warn me when sites try to install add-ons," "Block reported attack sites," and "Block reported web forgeries." I recommend avoiding both password options. As a general guideline, browsers aren't optimal tools for password management. There are other configuration settings that enhance privacy and security to be sure, but these few changes are enough to move us forward to the real breakthrough in personal privacy and security for browsers: the add-ons. Whereas the 1990s were characterized by the browser wars (for more, see www.berghel.net/col-edit/digital_village/oct-98/dv_10-98.pdf), we've now entered the era of add-on skirmishes.

The NoScript add-on

To start, I'm going to recommend two add-ons unreservedly—both offered though the Electronic Frontier Foundation (EFF), which has long been a leading voice behind the protection of civil liberties in cyberspace. The first is NoScript (see Figure 1), which is a dream come true for privacy zealots—it's a customizable, real-time, interactive script blocker that's also free. What a deal.

NoScript is designed to work seamlessly with scripting environments that operate with the more popular secure-sandbox-model virtual machines like Java, JavaScript, and Flash. I've had no problem with Adobe Reader, Acrobat, Silverlight, and Windows Media Player either. NoScript uses several innovations to get us around the problem where blocking the script renders the webpage unreadable. NoScript uses script surrogates that function essentially like the script embedded in the page, preserving usability and breaking nothing critical, but still disabling any nastiness. Script surrogates deal with page scripts of many ilk, including distracting "popunders" (aka "on-click" popups). NoScript is also effective at blocking cross-site scripting attacks and isolate IFRAMEs to prevent clickjacking. It also has HTTPS forcing as an option (which I don't use, as explained below). But even if NoScript breaks something, the configuration (NoScript Icon>Options) allows it to be tailored to suit the user's need. It can also be configured on the fly simply by selecting which of the scripts you want to run.

One of the best features of NoScript is its compatibility with other add-ons (and there are many good ones available). The latest version is 2.6.8.5 (see http://noscript.net). I should mention that silent running with NoScript comes with a penalty—users will have to go one extra step to temporarily enable scripts (individually or as a group) on script-hog sites, but that will give you the opportunity to reflect on whether that site is worthy of your interest after all. If you're interested in protecting your online privacy, this irritation is minor compared to the risk avoided.

The HTTPS Everywhere add-on

HTTPS Everywhere is a sister add-on from the EFF. This add-on only does one thing: it forces a Transport Layer Security/Secure

Sockets Layer (TLS/SSL) HTTPS connection if one is available on the server. It does this by means of the HTTP Strict Transport Security protocol (HSTS; RFC 6797). Of course, HTTPS is always preferable to HTTP where privacy is concerned, but until HSTS, the user had no way of knowing whether it was available. In addition, as Moxie Marlinspike showed in 2009, basic HTTPS could be vulnerable to a "SSL-stripping man-in-the-middle" attack, where a hacker could convert a secure HTTPS connection into an insecure HTTP connection without the user's awareness. Both the need of defaulting to HTTPS when possible, and preventing the Marlinspike hack are dealt with in HTTPS Every-where. In addition, the EFF builds in the SSL Observatory that monitors the use of HTTPS certificates on the Internet and provides warnings of possible attacks. Although NoScript also has HTTPS-forcing built in, its list-oriented configuration is more primitive and not as convenient as HTTPS Everywhere. HTTPS Everywhere v3.4.2.xpi is the current version for Firefox (https://www.eff.org/https-everywhere).

There are far too many good browser add-ons to describe in one setting, so stay tuned to this channel in *Computer* for updates. Remember that caveat emptor also applies with add-ons, as the code typically isn't validated by trusted third parties. For that reason, I recommend staying with add-ons written by the organizations you trust.

RAISING THE BAR FOR TELCO SNOOPS

Let's face it, the telcos have been illegally sharing our information with the government (and who knows who else) at least as far back as 1919, when Herbert Yardley formed his Black Chamber spy group after World War I. The big telcos of the day, Western Union Telegraph Company, Postal Telegraph, and All-American Cable Company, were then, as the big telcos are now, eavesdropping on US citizens on behalf of the government. The big difference is that these days the telcos spy with impunity.

Modern telcos aren't doing anything particularly unusual for their industry, and, likewise, the US government's eavesdropping on its citizens is also nothing new (Project Shamrock, Project Minaret, COINTELPRO). There have always been rooms like 641A somewhere. The recent twists are the Narus and Verint fiber-optic intercept suites and the optical fiber they work with. The stress testing of the Bill of Rights remains the same.

Hopefully, we'll all soon come to appreciate that the price for personal privacy is eternal vigilance!

The same applies to Wi-Fi—especially in metropolitan area networks. An alternative online magazine, *The Stranger*, recently exposed the Seattle Police Department's use of the infamous "white boxes" to intercept and store IP addresses, device types, applications running on the device, and location history data (www.thestranger.com/seattle/you-are-a-rogue-device/Content?oid=18143845). The "white box" project was funded by the US government (Department of Homeland Security), so it's unlikely that it's unique among metropolitan areas. The SPD apparently denied activating the white boxes until David Ham of Seattle's KIRO-7 News team asked why the wireless access point names were identifiable by smartphones (http://rt.com/usa/seattle-mesh-network-disabled-676). Another public deception over surveillance. Imagine that.

So, for you Seattle residents (and all you other white boxers out there), I have a few modest suggestions as well as some caveats. First, my remarks only apply to Android 2.3.3 on Casio 771/Verizon smartphones (the reader will have to extrapolate from there); second, the only effective countermeasure to undesired business and government eavesdropping and surveillance on cell phones is to "jailbreak" them to gain root privileges, and from root, block all of the intrusions from the carrier, Google, and the applications developers. I should note that the law in this area is magnificent in its disorder and continuously in flux.

To illustrate, the firmware in your smartphone is covered by the Digital Millennium Copyright Act (DMCA), which is interpreted every few years by the Librarian of Congress. In his most recent 2012 ruling, he opined that jailbreaking your smartphone will remain legal until 2015, but that unlocking a smartphone is illegal if it's done after 31 December 2012 (http://arstechnica.com/tech-policy/2010/07/apple-loses-big-in-drm-ruling-jailbreaks-are-fair-use). Note that under his penultimate opinion, the opposite was the case. Without rooting your phone, the telco can do/undo anything that you undo/do if it chooses, and if you do root your phone, a telco may develop an attitude and threaten to discontinue warranty service. So, at this writing, I'll take a swerve around jailbreaking and unlocking issues, leaving them to you and your attorney.

The security and privacy threats presented by smartphones and cell phones are real and should be taken seriously (www.zdnet.com/millions-of-android-users-vulnerable-to-security-threats-says-feds-7000019845). With these few caveats in mind, let's get into some privacy tactics.

I'll organize these suggestions by menu item. First, the telcos and their federal three-letter-agency partners have no business knowing where you are without your permission. So, let's shut off GPS services until we need them:

Settings>Location & Security

- VZW location services (uncheck)
- Standalone GPS services (uncheck)
- Google location services (uncheck)

Bear in mind that GPS 911 tracking won't be available with these services disabled, so if you're in a fix, you won't be able to tell 911 operators to "come find you"—you'll either have to tell them where you are or turn the GPS services back on.

Moving on:

Settings>Privacy

- Back up my data to Google servers (uncheck)

Backing up data to Google may be a really bad idea (see http://blogs.computerworld.com/android/22806/google-knows-nearly-every-wi-fi-password-world).

We continue:

Settings>Wireless & Networks>Mobile Networks

- Data enabled (uncheck)
- Global data roaming access—deny data roaming access (or "Allow access only for this trip")
- Wi-Fi (uncheck/off until needed)
- Bluetooth (uncheck/off until needed)

Settings>Accounts & Synch

- Background data (uncheck/off unless needed)
- Backup assistant (uncheck/off unless needed)
- Disable synch for all accounts

Settings>Applications

- Allow installation of non-market apps/unknown sources (uncheck/off)

Settings>Security

- Encrypt both device memory and SD card with different, long complex passwords that are different from the boot password

And when installing an application, carefully read the entire list of permissions required for it. If the app seeks permissions for camera, microphone, and so on, and you don't think that's reasonable, don't install it. Remember, the telcos operate under the caveat emptor rubric (and immunity!).

So there you have it. You've turned your smartphone into a paperweight. But it's a Constitutionally friendly, libertarian-and-privacy-pleasing paperweight that can make phone calls. That's not bad for a paperweight. And, of course, you can always turn these features back on and undo everything.

This primer barely scratches the surface, but it's … well, you know. Let me know what you think.

I would be remiss if I failed to again emphasize the obvious: the use of smartphones and the Web are, in and of themselves, invitations to privacy abuse. The widely available smartphone that's built around an encryption-based privacy model is the BlackBerry—which is precisely why it's unpopular in privacy-averse nations. The same applies to the use of social networking services like Facebook, Google+, Twitter, and LinkedIn, to name but a few, not to mention storing data on a cloud service. As Nicholas Weaver puts it, the government has weaponized the Internet (www.wired.com/opinion/2013/11/this-is-how-the-internet-backbone-has-been-turned-into-a-weapon), and unfortunately, there's a host of private cybermercenaries like ManTech, the Gamma Group, and Stratfor that are also in the mix (see www.washingtonpost.com/blogs/the-switch/wp/2013/11/04/yes-there-actually-is-a-huge-difference-between-government-and-corporate-surveillance/?tid=up_next).

But then the same may be said of the use of lower-tech credit and debit cards. Bankers, credit card vendors, and law enforcement agencies are all in agreement on one point: cash is the enemy of Big Brother.

Limiting use of such technology platforms and services isn't a product of technophobia or neo-Ludditism, but rather a defensive reaction to the rise of this modern "digital heel" that is used to control and manipulate the populace. These technologies are the grist for Orwellian and Huxleyan mills.

Those who persist at using privacy-revealing technologies and operating browsers in unsafe modes will probably not derive much benefit from the suggestions given here. But for the rest, this is a start. Those of us in the computing disciplines have been aware of security/privacy versus usability tradeoffs throughout our professional lives—some are more aware than others. What is new to this millennia is that governments have taken the leadership position in privacy and security abuses, from Stuxnet to tapping Angela Merkel's cell phones.

***Hal Berghel**, Out of Band column editor, is a professor of computer science at the University of Nevada, Las Vegas, where he is the director of the Identity Theft and Financial Fraud Research and Operations Center (http://itffroc.org). Contact him at hlb@computer.org.*