



Global Knowledge®

Expert Reference Series of White Papers

Technology Offers Convenience, Privacy Pays the Price

Technology Offers Convenience, Privacy Pays the Price

David Willson, JD, LLM, CISSP, Security+

Introduction

Today we are at a crossroads. Most of us value our privacy but also have succumbed to the allure of technological conveniences. With mobile devices, apps, social media and the Internet of Things (IoT) made up of smartwatches, smart TVs, smart cars, smart appliances, etc. so much of our privacy has disappeared.

Even if you are not concerned and value your technology and conveniences more than your privacy, you should consider the security issues introduced by the collection and availability of all of this information. Phishing attacks are becoming more and more sophisticated. Having all of our personal information online provides hackers the resources necessary to create very believable emails that trick us into clicking on links, responding, and providing more personal information or opening attachments and downloading malware.

Email phishing attacks are not the only threat. Today's technology and apps allow stalkers to more easily track their victims' whereabouts. Burglars can easily determine what valuables we possess and when we are not home. In order to protect ourselves and our businesses we must be able to recognize what information we are releasing, what is being collected, what is available, and who has access to it. This white paper merely touches the surface of this topic and does not begin to address topics such as the economic and social issues, including what information is available to potential employers, friends, dates, etc.

This white paper will review a few of the services many of us use; how information about us is collected, by whom, and for what reason; and some things we can do to limit that collection. To be clear, you can limit the information collected from this point forward but, for the most part the cat is out of the bag. In other words, there is a lot of information already out there available to almost anyone.

What is collected on us?

In reality, everything. Email addresses, email content, social security numbers, phone numbers, current location, shopping and buying habits, types of devices we use, our IP address, our contact lists, our names, current and all past physical/home addresses, place of employment, Internet browsing habits, mortgage information, criminal background, social media posts, photos, and the list goes on and on.

As revealed below, the amount of and frequency of collection is astounding. For instance, anyone can go online and do a background check on anyone else at sites like www.backgroundalert.com, which advertises 37 billion public records from thousands of federal, state, and commercial databases. Some of the information is free, but for a small fee you can dig deeper. A simple search will provide access to full contact information, criminal history, arrest history, traffic tickets, marriage records, divorce records, address history, known relatives, neighbors, and co-workers.

Most of us are familiar with and use apps on our phones and mobile devices. But we don't usually pay attention to the required permissions, instead just robotically clicking through and agreeing. So what are we agreeing to? LinkedIn, for instance, asks for permission to access phone status and identity; your precise location (GPS- and network-based) and to be able to modify your contacts. It also asks to read your call log, read your contacts, write to the call log, read your calendar and events plus confidential information, modify or delete the contents of your

SD card, read the contents of your SD card, add or remove accounts, create accounts and set passwords, find accounts on the device, gain full network access, receive data from the Internet, view network connections, control the phone's vibration, prevent your phone from sleeping, and more. Other apps, like Google +, want permission to take pictures and videos, record audio, access your photos, download files without notification, control the flashlight, set wallpaper, control audio settings, and much more. This is just a small sampling of the information collected about us.

Who is collecting?

As mentioned above, the list includes federal, state, and local governments, the app developers, and also, Internet Service Providers (ISPs), browser companies (Google, Firefox, and Yahoo), social media (Facebook, Twitter, LinkedIn, Snapchat, Instagram, etc.), background check companies, and services like Zillow, Spokeo, etc. So who is really doing the collecting and why? They are advertisers and those seeking to sell your information to them, who then target you with ads.

For instance, through a browser like Internet Explorer, advertisers are able to track your browsing activities. Recently Microsoft, claiming they needed to provide users a choice, changed their "Do Not Track" (DNT) policy from a default setting of "On" to "Off." Microsoft (MS) claims this allows the user to decide, but it also automatically allows advertisers the freedom to track. Implementing "DNT" will require action on the part of users and possibly some non-intuitive knowledge, thus most will likely not know about it and many of those who do will do nothing. Even if "DNT" is implemented, advertisers and others are merely requested by MS to honor this request.

As the IoT expands, more and more data about us is available and collected. "Google now has a new target: tapping, mapping and colonizing the networks wiring our lives."¹ Google recently acquired Nest, the company that sells Wi-Fi home-heating appliances. These devices allow the user to access them, via the Internet, from anywhere to monitor and control their home or business thermostat. Google collects data sent to and from these devices and argues, "[I]t has the right to collect your most sensitive data, as long as it flows across an open Wi-Fi network, . . ."² "Nest products track detailed information about their users' movements, in addition to things like a user's Wi-Fi IP address and whether the specific address is a home or a business."³

Some argue that another of Google's services used to invade our privacy is Street View. Google admitted, after a court challenge, that the vehicles driving around with roof cameras weren't just taking pictures but also "collecting data from computers inside homes and structures, including the 'passwords, emails and other personal information from unsuspecting computer users . . ."⁴ Google has also been sued for analyzing the contents of all of its Gmail users' emails and selling the data to advertisers. Gmail users as well as those they were emailing, even if that person was not a Gmail user, were then targeted with ads.⁵ Finally, Google apparently also knows nearly every Wi-Fi password in the world, having used backdoors and security workarounds on its Android operating system.⁶

¹ Rosenfeld, Steven, "4 Ways Google is destroying privacy and collecting your data," Salon, [HEREINAFTER 4 Ways] (Feb. 2014)
² *Id.*, See also, "Google says anything flowing across open WiFi is fair game," PrivacySOS: Sunlight on Surveillance, at: <http://privacysos.org/node/1299>.

³ *Id.*, at 4 Ways.

⁴ *Id.*, at 4 Ways, See also, NYT.

⁵ *Id.*, at 4 Ways.

⁶ *Id.*, at 4 Ways.

So as not to pick on Google, the article, "4 Ways Google is destroying privacy and collecting your data," highlighted other companies that spy on us. For instance, Dropbox, Microsoft, Apple, Yahoo, Facebook, and Skype, just to name a few.⁷ They all read user data and grant our government access to this data.⁸ Not to be left out, AT&T was sued and is paying a \$25 million settlement fine to the FCC for "leaking confidential information on about 280,000 subscribers so that resellers could unlock used phones, . . ."⁹ The disclosures included names, parts of social security numbers, and other data.¹⁰

How much is collected and how?

"Platforms, or operating system providers offer app developers and others access to substantial amounts of user data from mobile devices (e.g., geolocation information, contact lists, calendar information, photos, etc.) through their application programming interfaces (APIs)."¹¹ A recent study conducted by Carnegie Mellon University revealed the astounding number of times apps access information on peoples' phones. One individual participating in the study was told, "Your location has been shared 5,398 times with Facebook, Groupon, GO Launcher EX and seven other apps in the last 14 days."¹² Another participant stated, "It felt like I'm being followed by my own phone. It was scary. That number is too high."¹³

So, how is the data collected? Today, most of it is through electronic means, but some local government agencies and businesses, like medical offices, still collect data using paper forms. Information collected over the years by government agencies is now being scanned and put into electronic storage, which is all vulnerable to hackers, but more importantly, much of this data collected is publicly available.

Many of the electronic means of collection, as mentioned above, include the apps on our phones or mobile devices; the cookies on the browsers we use, like Google, Internet Explorer and Firefox; and our usage data collected by our Internet Service Providers (ISPs), our phone service providers, email providers, and the list goes on. Depending on the type of phone you use, the apps on that phone utilize the location services, your contacts, your browsing history, and much more to collect information. Sometimes this is done for your benefit and sometimes for theirs or advertisers.

⁷ *Id.*, at 4 Ways.

⁸ *Id.*, at 4 Ways.

⁹ Fitzgerald, Drew, "AT&T to Pay \$25 Million to Settle FCC Privacy Breach Case," The Wall Street Journal (April 2015)

¹⁰ *Id.* The identity of those who owned the phones and information to unlock them, in many cases, was sought by persons selling stolen phones. Cell phone service providers lock their phones so that they can only be used on their network, ensuring a two-year subscription for a reduced rate on a new phone. Consumer Reports estimates that 3.1 million smartphones were stolen in 2013 in the U.S. alone.

¹¹ "Mobile Privacy Disclosures Building Trust Through Transparency," FTC Staff Report (February 2013)

¹² Spice, Byron, "What Do You Do When Your Location is Shared 5, 398 Times?," Carnegie Mellon University, Forensic Magazine (April 2015)

¹³ *Id.*

Finally, what can we do about it?

How can we minimize the data collected, reduce our electronic footprint, and protect ourselves and our privacy online? Here are some tips and techniques you can use:

1. **Turn off the location services on your phone or mobile device.** If you need it at some point, for instance for maps or GPS directions, you can always turn it back on. As mentioned above, many of the apps that are preloaded or that we load onto our smartphones utilize location services to track our habits. Remember the Carnegie Mellon study in which one participant's location was collected more than 5,000 times in two weeks? Much of this data is then sold to advertisers. Free is good, but it does come with a price. One note of caution: A recent article notes that a California woman claims she was fired because she uninstalled the GPS tracker app on her company-issued iPhone when she found out that her boss was able to and did track her every movement, even when she was not at work and on her own time. She is suing, so this one will be interesting to watch.¹⁴
2. **Remove geo tags.** When taking photos, ensure there are no latitude and longitude or geo tags in the photos. When you post these photos to social media you are essentially advertising to others where the photo was taken. Recall the story of a man in Massachusetts who purchased a new big screen TV, took a photo of it at his house, posted it on Facebook, and then announced he was going on vacation. While on vacation his house was robbed and his TV stolen. For most phones or mobile devices, disabling "location services," as mentioned above, will take care of this. You can also open the camera app and disable geo tagging in settings.¹⁵
3. **Freeze your credit or have it monitored.** Identity theft due to credit card and other data breaches has become a huge problem for the consumer. Many people sign up for one of the paid services that monitors their credit, but, if you don't want to pay, you can also freeze your credit. This may not be as extensive coverage as with a paid service, but is certainly better than nothing. Simply go to the three credit bureaus—Experian, TransUnion, and Equifax—and submit the required information to freeze your credit. This will prevent others, for the most part, from viewing your credit and opening accounts or taking out loans in your name. If you need to take out a loan or someone needs to review your credit you can always unlock it.
4. **When using social media, read and implement all privacy features.** Most social media services, which are free and make money from the sale of advertising, provide privacy features. Be cautious though since some social media providers, like Facebook, will change these features frequently, disabling your privacy, so you need to constantly check these settings. Again, remember, they make money by selling advertising through tracking your habits, likes, dislikes, and other information, which allows them to create targeted ads.
5. **Use an anonymizer when browsing.** "An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable."¹⁶ There are many free add-ons you can use on your browsers, such as OpenDNS, Hotspot Shield, Hide My Ass, and others. The Onion Router (Tor) was and continues to be used by many, especially hackers, to hide their tracks online. This free service bounces your IP address around so your location cannot be tracked. It also can encrypt the data you are sending and receiving. Tor has had many issues lately, so it is recommended you do some research before implementing it.

¹⁴ Kravets, David, "Worker fired for disabling GPS app that tracked her 24 hours a day," *ars technica* (May 2015).

¹⁵ "Police: Thieves Robbed Homes Based On Facebook, Social Media Sites," *WMUR 9 ABC*, (Sep. 2010), at: <http://www.wmur.com/Police-Thieves-Robbed-Homes-Based-On-Facebook-Social-Media-Sites/11861116>.

¹⁶ "Anonymizer," *WikiPedia, The Free Encyclopedia*.

6. **Don't use public Wi-Fi.** Public Wi-Fi at airports, hotels, coffee shops, and other places is easily monitored by hackers and those seeking to steal information. A better option is to tether your phone to your computer or create a secure hotspot with your phone to which only you have access. In other words, don't set up an open hotspot without a password since anyone can then connect to your network. By using these options you will be accessing the Internet through the cell tower system rather than through public Wi-Fi. The cell towers are a more secure option.
7. **If necessary, use a VPN.** A virtual private network, or VPN, is like a tunnel for communications. If you are sending messages via email or other means and need to keep them secure, a VPN will allow you to do this. In most cases though VPNs require a paid service and you have to set it up between yourself and the person to whom you are sending messages. Picture it as similar to the old string-and-can technique.
8. **Don't put sensitive data in the cloud unencrypted.** Unless you are aware or receive a guarantee from whomever manages the cloud service that they have never and will never be breached, make sure you use encryption. Additionally, read all of the agreements before signing and make sure you know what the provider is responsible and liable for and what security they provide.
9. **Use two-factor authentication.** Many providers, such as Google, offer this service. An example is, as you log on and enter your username and password, a one-time code or pin is texted to your mobile device. Once you enter this code you are provided access. This provides another layer of security since, in most cases, someone who has gained access to or stolen your username and password will not usually have access to your phone and receive the one-time pin texted to you.
10. **Block third-party cookies.** Cookies are pieces of code set on your browser by websites you visit in order to track your browsing history and target you with ads. They may also be used to determine your location based on your IP address. Many websites will not load unless you enable cookies. Third-party cookies, similar to cookies, are placed on your browser by a website that is merely a part of the website you are viewing, or a third party to that website. For instance, if a website you are viewing has a Facebook button, Facebook may attempt to install a third-party cookie. In order to disable third-party cookies and other unwanted services, review the settings on your browser. There are many options for you to customize.
11. **Use a proxy or VPN to block your IP address and avoid location tracking from your browser.** As mentioned above, there are various apps, add-ons, and software you can use that will mask your IP address. Even though your IP address, in most cases, can only indicate what city you are in, blocking it will help avoid tracking and ads targeted for your location.
12. **Use the "Do Not Track" (DNT) function available in some browsers.** As mentioned, Microsoft has disabled "DNT" as the default, but you can enable it. This does not mean websites cannot track you, but it tells them you do not wish to be tracked.
13. **Manage plugins.** Some browsers, like Chrome, allow you to request a notification whenever the plugin is asking for information. Firefox, when downloaded and during use, will frequently install add-ons without asking your permission. Whatever browser you are using, make sure you review the settings and customize for your preferences.
14. **Disable Javascript or use a service that manages it.** Javascript is a powerful computer language utilized by most web browsers and manipulated by many hackers. You can disable it but some functions, like videos, may not work properly. Disabling Javascript is a choice you will need to make. If you go a few days without it and don't notice any problems, then leave it disabled. Sites requiring it will let you know.

15. **Use HTTPS everywhere.** HTTP is a language websites use. The "S" in HTTPS stands for "secure" and ensures that websites are verified and the transfer of data is secured, for the most part.
16. **Use Ghostery Browser extension.** Ghostery is a free add-on available for most browsers. It helps you to block websites and others seeking to track you and your habits.
17. **Use Panoptick or similar service to check what info your browser is collecting.** This site will scan your browser and reveal to you how unique your settings are. If they are common, then you are likely being tracked like most.
18. **Use virtual machines.** Virtual machines are actually virtual operating systems you can set up on your computer or servers. It is recommended that virtual machines be used for logging into sensitive sites like banks since once closed, the virtual machine can be deleted. In this case, each time you open a virtual machine you know that it is clean and virus-free.
19. **Use a throw away email address.** When signing up for online services and other sites, use a different email address from the one used for work, friends, banks, and other important services. Therefore, most of the spam you receive will go to these accounts, which you can ignore. Potential viruses and malware that may infect your computer can be limited since you will rarely open this account on your computer and can avoid opening emails from this account knowing they are likely junk.
20. **Avoid unsubscribing from unwanted emails you receive.** Frequently we all receive unwanted emails. In many cases these emails are not legitimate but are from spammers. They are hoping you respond or unsubscribe. When you respond you legitimize your email address and it is then put on a spam list. If you receive unwanted emails, either merely delete or block the emails. If you continue to receive them six or more times, then it may be safe to unsubscribe as the emails are likely legitimate.
21. **Limit the information you provide.** When signing up for social media and others sites, limit the information you provide or use fake information. Most sites require you be truthful, but you can omit much information in order to limit what is available about you.
22. **Set up Google Alerts for your name.** Google Alerts is a service that will provide daily alerts about various topics based on key words. If you set up a Google Alert with your name you will receive a notice every time your name appears online. This will help you know what information is being posted about you.
23. **Use fake answers to the security questions.** When signing up for accounts, if asked to establish answers to security questions, use fake answers. This way it will be impossible for someone to guess your answers based on information they learn about you online or via social media.
24. **Use a Skype or Google phone number instead of your actual phone number.** Similar to a fake or throw-away email account, sign up for a free Google or Skype number and use this when signing up for various sites. This will help you to avoid robocallers or solicitors.

Conclusion

Technology is a wonderful thing, but it comes with a price. Much of the data collected about us is done so for a legitimate purpose—advertising. We may not like it, but if we continue to expect services for free it is only logical that those providing that service make money one way or another. In the many articles I read while researching this topic, many people commented that they would be willing to pay for many of the services in order to limit the collection. I think that ship has sailed. If companies thought they could make more money selling their service versus selling our data to advertisers, they would have likely done so already. Probably the best we can hope for is that with enough attention focused on privacy that those providing services would offer an option to those interested. For instance, pay and protect your privacy, or accept the service free and agree to the collection of data. More important than how much and what is collected is who has access to it and what they do with it. This is why you should take steps to limit the data collected and how it is used, and monitor the information available about you.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

[Legal Issues in Information Security](#)

[Cybersecurity Foundations](#)

[CyberSAFE \(Securing Assets for End-Users\)](#)

Visit www.globalknowledge.com or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

David is an attorney and an expert liability management and cybersecurity consultant, licensed in New York, Connecticut, and Colorado. He helps companies understand the liability associated with information security and data breaches. He also assists law firms with technical litigation, electronic evidence discovery, and the introduction of this evidence. He has worked in information security for more than 15 years and has written and provided lectures in this area over the last three years. David is a retired U.S. Army JAG officer. During his 20 years in the army he provided legal advice in computer network operations, information security, and international law to the Department of Defense (DoD) and National Security Agency (NSA) and was the legal advisor for what is now CYBERCOM. He has published many articles, spoken at many conferences, and conducted numerous classes and training in risk management.