©blackday | AdobeStock

A Beginner's Guide to Surveillance, Digital Security, and the Privilege

As anyone who can spell "Internet" must know by now, when we use digital devices for work or play, we are subject to the compromise of our communications and stored information by way of government, corporate, or criminal interception and surveillance. With our fingers on the keys only a few inches from our screens, the relationship between ourselves and our computers seems as intimate as lovers sitting side by side on a park bench. Intellectually, we know that the Internet is the nervous system of a wired world, where what we ping, pings us. What we do not fully absorb is how those wires wind together to form a sieve through which our digital self-expression is emptied into the waiting hands of strangers, eager to exploit it to ends we can barely imagine.

To participate in the commerce of the Internet, we must become its currency, exchanging our privacy for the barter of goods, gossip, news, and entertainment. The subtle compromise of our privacy makes it easy to forgive the invasion. The relentless cataloging of our clicks on every website, of every document we open, of our text and voice communications, every purchase, and each news item we peruse, is conjoined to similar life logs of all other users in a mosaic of our emotional, intellectual, and commercial experiences. The sum total of all our past choices and comments is the predictable trajectory of all our futures. Possessing predictive data on our billions of futures has unparalleled commercial and political value.

The scope of this commercial surveillance far exceeds that of any past totalitarian governments, but pales in comparison to the surveillance reach of our own. The government of the United States has declared eminent domain over all our secrets. It alone combines web-based surveillance with the global interception of personal, commercial, and governmental communications, international and domestic signals traffic, and by either legal or extralegal means, the proprietary data traffic of private industry and technology companies. Other governments are now striving to follow our example.

Even though we have a general, if uncomfortable, awareness of the promiscuous exploitations of our every digital transaction, we tend to behave more like customers than lawyers. In the trivial remarks we post, in the emails, texts, and Facebook messages we send, the "likes" we click and the products we buy, we believe we have done nothing worthy of the government's gaze. We have nothing to hide. Nothing we do on the Internet or with our digital devices violates the law, and therefore, we are not targets of surveillance.

Yet every one of us would tell even our most certifiably innocent client not to make a statement or allow a search without a warrant based upon the client's confidence that he or she has "done nothing wrong." We give this advice because our training and experience have

BY SAM GUIBERSON AND JEREMY GILLULA

taught us that the true motives of a criminal investigation are not initially made apparent to the suspect and that the stated superficial objective may be quite different than the suspicion or evidence left undisclosed. So it is with digital surveillance. The essence of mass surveillance is that no target is less a target than any other.

The gargantuan scale of the surveillance governments now undertake advises us that strategic and predictive intelligence is more valuable than criminal evidence. Presuming falsely that mass surveillance is just a world wide web of stoplight cameras built to catch those who run red lights, we operate our digital lives on the assumption that the sole objective of mass surveillance is to document evidence of culpability, when the true objective of mass surveillance is to control by the exploitation of secrets.[1] There may well be a ghost in the digital surveillance machine, but unfortunately for us and for our clients, it is Machiavelli's ghost.

We cannot neglect our duty to protect the attorney-client privilege merely because our professional communications are immersed in a multiplex of digital surveillance technologies. Our decisions about our personal digital privacy need to be segregated from those we make when we bear responsibility for our clients' privacy, security, and legal defense. No personal decision an attorney makes is substitute for a disciplined, well-informed assessment of the risks posed to a client's privileged communications. As individuals, we can choose to negotiate away our privacy. As lawyers, we must defend a client's privilege absolutely.

Intelligence Standards and Standards of Ethics

In a surveillance state, is there a tension between the State and the attorney-client privilege? Is there even such a thing as client confidences and effective assistance of counsel if the State, at its discretion, may harvest a rich portfolio of attorney-client communications, attorney web searches, and call data records of a law office by means of dragnet interception? In our emergent surveillance state, there is reason to believe that half measures of compartmentalization exercised subsequent to mass collection constitute our government's best efforts to recognize the attorney-client privilege.

In 2014, on the heels of the Snowden disclosures of the massive scope of NSA surveillance, then-American Bar Association President James Silkenat wrote a letter of concern to General Keith Alexander, then Director of the National Security Agency, regarding the reported interception of an American law firm's communications with its foreign client by Australian intelligence with the NSA's collaboration. The intercepted communications from that surveillance were then offered to the NSA under a long-standing reciprocal intelligence sharing agreement among countries known as the "Five Eyes."[2] The compromised privileged communications related to a trade dispute involving clove cigarettes and shrimp pricing, a matter in arbitration between Indonesia and Australia at the time.[3]

General Alexander responded with due deference to NSA's legal obligation to prevent the unrestricted use of attorney-client communications occurring post-indictment after the right to counsel had attached. He cited the minimization procedures set out in Executive Order 12333[4] and Section 702 of the Foreign Intelligence Surveillance act, the statutory cornerstone for court authorization of mass surveillance of international communications, including participating domestic U.S. persons. The NSA director also described a construct of procedural safeguards that would meticulously compartmentalize intercepted attorney-client communications of which the Agency has notice by means of court records.

The Porous Quarantine of Intercepted Privileged Communications

Even assuming that NSA would strictly quarantine collected attorney-client communications, but for the "foreign intelligence information contained therein,"[5] the exceptions may swallow the rule.

At the pre-indictment stage of criminal representation, the identities of counsel not of record and all members of the defense team are opaque to a federal database of only indicted defendants. No provisions are in place for identifying or segregating communications with counsel pre-indictment, or for defense team members who are not named counsel in court records upon which the NSA will rely. Quarantine of only attorney-client communications that occur *post-indictment* conflates the right to an attorney with the right to the attorney-client privilege. NSA sequestration or minimization of only an indicted defendant's communications with counsel provides only a hollow deference to the much broader actual scope of the privilege.

The additional carve-out of preserving attorney-client communications that contain "intelligence information," or when collectors are given other advice "tailored to the particular facts and circumstances in which sensitive intelligence activities have been or are to be undertaken,"[6] begs the question of how intercepted privileged communications can be exploited as intelligence outside the walls of the courthouse in a criminal prosecution. Are they available to blackmail an American or foreign citizen to work as a spy or as an informer? Can they be used to investigate criminal enterprises or drug trafficking conspiracies as long as privileged source intelligence is disguised so that it is not identifiable in a criminal prosecution? Are they available to leverage favors from politicians, executives, or professionals when a highly confidential and sensitive government request is made? There are many ways in which inventive minds can exploit the interception of privileged communications to the disadvantage of a client without allowing the sun to shine upon that surveillance in a court of law.

If our intelligence and law enforcement agencies' situational and opportunistic calibration of the term "sensitive intelligence activities" can include a defense counsel's representation of a Guantanamo detainee on the one hand, and a lawyer handling Australian shrimp import negotiations on the other, there must be a very flexible standard for what legal representation may be postulated as having intelligence value.

And yet, no matter how circumscribed the U.S. government's intelligence cache of attorney-client communications may be, its intelligence-sharing partners and every other surveillance operator, whether state sponsored or not, are under no such constraints in their exploitation of privileged communications.

The Guidance of Professional Ethics

In August 2013, the ABA House of Delegates issued a new policy statement[7] condemning "unauthorized, illegal governmental, organizational, and individual intrusions into the computer systems and networks utilized by lawyers and law firms" and opposing "governmental measures that would have the effect of eroding the attorney-client privilege, the work product doctrine, [and] the confidential lawyer client relationship. …" This statement also urged compliance with the ABA's Model Rules of Conduct, updated in 2012, to include changes to Rule 1.6 "Confidentiality of Information," stating that "a lawyer shall make reasonable

efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[8] The use of the imperative obligates attorneys to maintain such expertise as is necessary to make efforts that are "reasonable" to insure there is no disclosure of, or access to, information relating to representation. This standard of practice compels reasonable measures be taken to defeat covert mass surveillance and cyberattack which, by definition, are not authorized by the client. And yet, within the single word "reasonable," there is a mansion with many rooms of wiggle.[9]

In a 2012 NACDL Ethics Advisory Committee Opinion issued in response to restrictions on attorney-client communications arising from the Guantanamo Tribunals, the committee decided that "without the client's informed consent, a lawyer cannot communicate with his or her client, or record and preserve communications with the client, or create and preserve other written work product, in a manner that allows others to have access to the communications."[10] The implication of this opinion in a mass surveillance context would seem to be that absent the client's consent, a criminal defense lawyer cannot ethically represent a client when he or she cannot effectively prevent government or private actor surveillance access to privileged communications and preserve the cybersecurity of work product. In another related ethics opinion, the Advisory Committee stated, "A criminal defense attorney has an ethical and constitutional duty to take affirmative action to protect the confidentiality of attorney-client communications from government surveillance."[11] Or, put another way, when it comes to the defense of the privilege against government surveillance or cyberattack in criminal practice, to quote Yoda, "Do, or do not. There is no try."

It Takes a Village to Protect the Privilege

Governments can vacuum up our privileged communications, but the privilege cannot be defended in one. Lawyer and client must agree on what standard of communications security and data protection will be appropriate to the risk profile of the case, and then get buy-in from other members of the defense team. One new dimension of law practice, in this era of so many "eyes" and "ears," is counseling clients and negotiating agreements among co-counsel, and even with co-defendants' counsel, as to what level of operational security can be successfully applied when vigorous precautions are required. Total unanimity of action in the defense camp is essential to protecting privileged communications and work product.

Today, the expense of employing most of the capable security measures described in this article is not a deterrent, but the challenge of applying them may well be. As surely as there is a learning curve in applying technology-driven countermeasures, there is a learning curve in successfully adapting to privilege-protective practices that were utterly unfamiliar to lawyers before the full scope of mass surveillance was well understood. All clients in all cases do not require the same technical measures or the same degree of vigorous protection. In assessing what particular facts enhance the prospect of defense team communications and computer files being targeted, it is important to understand that there is more than one dragnet.[12] Trying to anticipate every possible threat is like trying to hold on to your wallet at a pickpockets' convention.

Surveillance Risk Management

A lawyer must speculate on who are the more probable aggressors, because surveillance technologies, cyberattacks, and intrigues[13] that can compromise a client are not so sophisticated that only the U.S. government can deploy them. Our privileged communications are also subject to attack from other governments' hackers, crime syndicates, drug cartels, a client's business or political adversaries, international and domestic crime syndicates, or contract hackers seeking business intelligence or blackmail in discovery files, or just to turn a profit with inside information about a celebrity defendant or a highly publicized case. Evaluating whether any of these risk factors are in play, quite aside from apprehensions of NSA or law enforcement surveillance, will shape the defense team's response in mounting its own security practices. The old Watergate adage "follow the money" is a good place to start; who benefits by disclosure or exploitation of the accessed information? It is clearly not the world of our childhoods when the practice of law draws closer and closer to the practice of espionage.

The types of cases in which it is reasonable, if not essential, to undertake countermeasures to defend privileged communications are those involving investigative activities or contact with individuals outside the United States. It is also worth evaluating the international political profile of the case. Does an acquittal or a conviction impact the reputation or credibility of any government, a political party, or business interests intrinsic to the power structure of a foreign country? Does the client have, or could it be believed that the client had, some information that would compromise such financial, political, or criminal interests? Is there a criminal organization, or a domestic or foreign political organization, or a major foreign or domestic corporation, which is likely to be implicated or communicated within the course of the defense? Will a successful defense or prosecution affect the value of any public company that has competitors or takeover raiders snapping at its heels? Cases that involve foreign nationals with organized crime ties of even the most modest variety may draw the interest of their home countries as well as their homies.

Another category of high risk are those offenses in which some element of the United States government perceives itself as the victim, or perceives its foreign allies to be victims, or in which the unsuccessful prosecution of the case would affect national interests or political reputations. A related class of potentially high risk cases is that group in which the contents of the government discovery, or of the defense investigation, would have political, commercial, or intelligence value, or when its exposure would affect the reputations of powerful government, corporate, or international figures or families.

The intelligence community's license to share criminal intelligence with federal law enforcement agencies, and the inevitable trickle down to state agencies through joint task forces[14] and fusion centers,[15] broadens the implications and the consequences of privileged communications surveillance in routine criminal practice. Police priorities, political priorities, and publicity priorities all skew the incentives toward using surveillance-based criminal intelligence far from the realm of espionage and terrorism cases. The use of parallel construction[16] to cloak any linkage of the actionable intelligence to mass surveillance sources gives cover and encouragement to local law enforcement by assuring that

any well-concealed violation of privileged communications is never put before a court.

Just as a national security agenda may "trickle down" to investigations at a local police level through Joint Task Forces and Fusion Centers, so too can a local security agenda "trickle up" to gain sanction for the robust use of surveillance directed at local threat priorities identified by local police. Local police suspicions and resentment of local leadership in communities of color; social justice, peace, and environmental activists; and even animal rights activists have historically experienced intense surveillance and infiltration from local and federal law enforcement using the full array of technologies available at the time. In the quid pro quo relationships existing between federal and local law enforcement agencies, the surveillance tools designed to defend the national security are often deployed in defense of the status quo. When the client is an individual whom police associate with a dissident local group espousing radical politics, social justice, racial, anti-war or anti-capitalist sentiments, there is substantial risk of physical, digital, and communications surveillance, on or off the ledger of accountability to elected officials.

There are also dire consequences for a defendant when a confidence meant for his attorney finds its way to law enforcement agencies that act upon that tip from an undisclosed surveillance interception. Persons not under suspicion may suddenly find themselves targets and logically conclude that the client has informed on them to law enforcement, rather than having only informed his attorney. The exploitation of intercepted privileged communications in organized crime cases, drug conspiracy cases, gang-related cases, and terror prosecutions can all lead to a snitch's fate for a defendant who breached no trust with his fellow conspirators, but trusted his lawyer. Equally sobering is the prospect that these unknown third parties with anger management issues may hold the defendant's attorney liable for their compromise.

When one or more of these factors is integral to a case, there exists a credible risk of persistent, aggressive surveillance from one or more of these many actors. It is always lawyerly to admit that our best professional insight may be inadequate as to what factors in a case focus clandestine surveillance upon the defense. What we guess, what we presume, and even what we know about our case facts, may fall short of what those with the power to surveil or to hack us consider valuable to their own ends. Our footprints in the digital snow, as well as our clients', may lead to consequences we simply cannot anticipate. The default practice should be to leave as few footprints as possible.

Surveillance Defense Technology and Practice

Protecting communications, documents, and Internet usage from bulk surveillance and targeted attacks requires a broad spectrum of security-enhancing tools.

It is critical to remember that security is a process, not a purchase. No tool is going to give you absolute protection from surveillance in all circumstances. Using encryption software will generally make it harder for others to read your communications or rummage through your computer's files. Attacks on your digital security will always seek out the weakest element of your security practices. The tools and practices recommended below have been chosen to maximize the security benefit they provide, while minimizing the effort required to use them.

Using Strong Passwords and a Password Manager

The first task in securing your digital world is to start using strong passwords. Almost every online service, not to mention every form of encryption, relies on some sort of password — which makes your password the first thing an attacker will try to break. And attackers have an advantage: computers are now fast enough to quickly guess passwords shorter than ten or so characters, even totally random ones like "nQ\m=8*x" or "!s7e&nUY."

So how do you select a strong password? The most straightforward method is Arnold Reinhold's "Diceware" method.[17] Diceware involves rolling actual physical dice to randomly choose several words from a word list; together, these words form what is called a passphrase. The benefit of this method is that random words are a lot easier to remember than random characters, and you need fewer of them: a six-word passphrase can be stronger than a 12-character password, because there are a lot more words to choose from than there are characters (even if you include upper and lowercase, numbers, and symbols) so it is harder for an attacker to try all the possible combinations of words.

Of course, it is important to never reuse a password on different services because if an attacker gets hold of one password, she will often try using that password on your other accounts. If you reused the same password several times, the attacker will be able to access each account where it was reused. That means a given password may be only as secure as the least secure service where it has been used.

That's all well and good, but how are you supposed to remember dozens of different passwords? Fortunately, you do not have to. There are software tools — called password managers (or password safes) — that can protect all of your passwords with a single strong master pass phrase, so you only have to remember one thing. This makes it practical to avoid using the same password in multiple contexts. In fact, if you use a password manager, you no longer need to even know the passwords for your different accounts; the password manager handles the entire process of creating and remembering them for you.

The Electronic Frontier Foundation (EFF)[18] recommends KeePassX,[19] which is a free and open source password manager. KeePassX works with files called password databases, which are exactly what they sound like: files that store a database of all your passwords. These databases are encrypted when they are stored on your computer's hard disk, so if the computer is off and someone steals it, they will not be able to read your passwords.

Note that KeePassX does not have a built-in sync feature — it won't automatically sync your password database between different devices. So what if you need your passwords on more than one computer? *As long as you use a strong master passphrase*, it should be relatively safe to sync KeePassX's password-database file to other devices using any cloud-based service (Dropbox, Google Drive, etc.). That's because the password-database file is encrypted using your master passphrase, so even someone who gets access to your cloud sync service will not be able to read your passwords. (It's worth re-emphasizing the importance of using a six-or-more word passphrase if you're going to sync your password-database to the cloud.) And if you need your passwords on your smartphone, there are also KeePass clients for Android and iOS.

Encrypting Your Devices

Now that you know how to pick a strong password and store all your passwords securely, the next step to main-

taining attorney-client privilege is to ensure that your files and documents are safe at rest — i.e., when they are stored on your computer or smartphone so that a lost or stolen device is not an open book for a would-be thief.

It is safest and easiest to encrypt all of your data, not just a few folders. Most computers and smartphones offer complete, full-disk encryption as an option.

If you use a Mac, chances are your computer is already encrypted: versions of OS X 10.10 and later ("Yosemite," "El Capitan," and "Sierra") all enable disk-encryption by default using a tool called "FileVault."[20]

If you use a PC, Windows calls its encryption system "BitLocker." BitLocker is built in to Windows 7, 8, and 10, but only the non-Home editions (e.g., Windows Professional or Enterprise). It's not necessarily enabled by default, so you may have to enable it.[21] Some PCs don't support BitLocker — in that case, you can try using a free, open-source tool called DiskCryptor.[22]

In addition to computers, smartphones (which are basically tiny super-portable computers, after all) should also be encrypted. If you have an iPhone 3GS or later, an iPod touch 3rd generation or later, or any iPad, you can enable encryption. In fact, most modern Apple devices encrypt their contents by default, with various levels of protection.[23] You can also encrypt Android smartphones running Android Gingerbread (2.3) or later. Some smartphones running Android Lollipop (5.0 or higher) will have encryption enabled by default.[24]

Whatever your device calls it, encryption is only as good as your password. If your attacker has your device, they have all the time in the world to try out new passwords. Forensic software can try millions of passwords a second. That means that a four number pin is unlikely to protect your data for very long at all, and even a long password may merely slow down your attacker. Thus, you should use a nice, strong, six-plus word diceware passphrase when encrypting your computer — and at least a six-digit PIN code for your smartphone.[25]

It is also important to note that even if your device is encrypted, an attacker may be able to get around that encryption and access your files via any backups you regularly make. If your backups are to the cloud, the connection between your device and the cloud will almost certainly be encrypted, so you do not have to worry about information being leaked as it is being sent and received. However, it is possible that the backup itself may not be stored in an encrypted manner, and thus anyone with access to your cloud backup account could access your files (or a government could pressure the service to turn them over). To avoid this weakness, make sure to choose a cloud backup provider that encrypts the data before it leaves your computer (sometimes known as a zero-knowledge system, since the provider has "zero" knowledge about your files).

Alternatively, if you back up to a local device (like an external hard drive), just make sure that device is also encrypted.[26]

Finally, note that encrypting an entire disk for the first time may make a device (be it your smartphone or computer) slower than usual for several hours, so we recommend starting this process before going to sleep, or letting it run over the weekend. Once the initial encryption process is complete, however, you should not notice much of a performance difference for most modern devices.

Browsing the Web Securely (and Anonymously)

When it comes to browsing the web, there are three major ways modern technology leaks information to attackers or government agencies.

The first privacy leak comes from the fact that not all communications between your computer and the websites you visit are encrypted. In other words, when you tell your browser to fetch a webpage for a given website, that request, and the page the website sends back, are not necessarily encrypted. This means anyone who can intercept the traffic between your computer and the website (including government agencies, but also anyone nearby if you're using an open Wi-Fi connection) can see what you are reading, as well as any information you might send back.

Of course, many websites *do* use encrypted connections — banks and web-based email providers, for example, almost certainly use encryption. But how can you tell? Look for an "s" after the "http" in your browser's URL bar. If it says "http://", it is not encrypted. But if it says "https://", the connection is encrypted.

Unfortunately, there is not much you can do if the connection is not encrypted; websites have to proactively offer encryption, and you cannot force a website to upgrade to an encrypted connection if the website does not support it. Sometimes, however, a website will support encrypted connections, but not use them by default. To deal with that case, you can install one of EFF's browser add-ons, HTTPS Everywhere. HTTPS Everywhere is available for Firefox and Chrome browsers, and will automatically upgrade your connection to a secure one on any website that supports it.[27]

All the encryption in the world will not help with the second privacy leak, which is third-party tracking. When you view a webpage, that page will often be made up of content from many different sources. For example, even though only one address will show up in your browser's URL bar, a news webpage might load the actual article from the news company, ads from an ad company, and the comments section from a different company they have a contract with to provide that service. If you visit lots of different websites, and those different websites all use the same ad provider, then that ad provider can track you as you browse the web — often without your knowledge.

To block this non-consensual third-party tracking, EFF has another browser add-on for Firefox and Chrome, called Privacy Badger.[28] Privacy Badger stops advertisers and other third-party trackers from secretly tracking where you go and what pages you look at on the web. If an advertiser seems to be tracking you across multiple websites without your permission, Privacy Badger automatically blocks that advertiser from loading any more content in your browser. To the advertiser, it is as if you suddenly disappeared.

However, neither encryption nor blocking third-party tracking can prevent the final privacy leak, which is the fact that when you visit a website, the website itself knows you visited and can track your subsequent visits. Additionally, anyone who can intercept your traffic will be able to tell when you visit that website and for how long, because while *what* you send or receive may be encrypted, the *identity* of the website you are visiting is never encrypted. Once again, that means that aspects of your browsing activity are susceptible to bulk surveillance — as well as anyone who can pressure your Internet service provider into watching your traffic.

To plug this privacy hole, you can use the Tor Browser.[29] Tor Browser works just like other web browsers, except that it sends your communications through a network of volunteer-run computer relays, making it harder for people who are monitoring you to know exactly what you're doing online, and harder for people monitoring the sites you use to know where you're connecting from. Keep in mind when using Tor Browser

that only activities you do inside of Tor Browser itself will be anonymized. Having Tor Browser installed on your computer does not make things you do on the same computer using other software (such as your regular web browser) anonymous. And of course, logging in to a site like Facebook or Google via Tor Browser will enable those services to track you anew for as long as you keep Tor Browser open.

Communicating Securely

Communicating is probably the most difficult task to accomplish securely because you have to coordinate with whomever it is you are communicating. Fortunately, there are some software tools out there that make the process a little less painful.

Let's start with text messages and instant messaging apps. Generally speaking, neither text messages nor instant messages are encrypted — which means anyone who can see the messages as they travel between your smartphone and your client's smartphone can read them — particularly government agencies that perform bulk surveillance. Some instant messaging apps — Google Hangouts, for example, or Facebook Messenger — do encrypt the messages in transit, but they have to pass through a central server, where they are temporarily decrypted (and often recorded). As a result, anyone who can hack your account (or pressure the company into turning over data) can read your past messages. Very few instant messaging services actually provide what is known as end-to-end encryption — named thus because the messages are encrypted at one end of the communications channel and are not decrypted until they reach the other end. Only end-to-end encryption ensures that only you and your client can read your messages.

One of the few choices out there for end-to-end messaging is an app called Signal, available for Android and iOS.[30] Signal not only encrypts your text messages (to other people using Signal on their smartphones), it also allows you to make encrypted voice calls.

Unfortunately, email encryption is a little more difficult. By default, email is not encrypted when you transmit it over the Internet — it is like a postcard, readable by anyone who handles it. Depending on which email provider you use, parts of the delivery channel may be encrypted. For example, most web-based email providers (Gmail, Outlook, etc.) encrypt the connection between your computer and their server. But once your email leaves their servers, it may or may not be encrypted any longer.

To get around this, you need a system that encrypts your email — essentially an encryption "envelope" you can drop your message into. The most common system is called "PGP." It takes quite a bit of work to set up, and you have to use desktop or app-based email software to actually read your email, but the results — totally secure, seamless email encryption — are well worth it.[31]

Alternatively, if PGP proves too daunting, you can fall back on a more ad-hoc system to communicate securely over email. For example, you could agree on a specific, strong, shared passphrase ahead of time with your client.[32] Then, to send a message to your client, you can write your message in a text (or Word) document (instead of in the body of an email), encrypt the document via a program like 7-Zip for Windows[33] or Keka for Mac OS X[34] (using the passphrase you agreed on ahead of time), and then send the encrypted document as an attachment to an email. Your client then simply has to download the attachment, and extract the document (using the shared passphrase you agreed on ahead of time).

It is important to note that a system like this has some down sides. For example, PGP allows you to verify the identity of whoever sent you an email, but in this system, anyone who discovers the shared password could impersonate someone else and send an encrypted message. Additionally, 7-Zip's encryption code has not necessarily been vetted in as much detail as the code in tools like PGP designed specifically for secure communication. With that said, while such a system might not be "NSA-proof," it's probably sufficient to keep a purely passive adversary from reading your conversations.

The Insecure Security Future

As it is with technologies, so it is with surveillance. The only constant is constant change. To maintain the security of attorney-client communications and defense work product, criminal defense lawyers must keep alert for news of evolving surveillance threats and new privacy countermeasures. The relative safety of software and computing devices is constantly shifting as new flaws are discovered and old bugs are fixed. Companies may compete with each other to provide you with better security, or they may all be under pressure from governments to weaken that security. It is also important to note that no software or hardware is entirely secure. Software companies that are honest about the limitations of their products will give you reliable information about whether their application is appropriate for you.

Do not trust blanket statements that say the code is "military-grade" or "NSA-proof"'; these mean nothing and give a strong warning that the creators are overconfident or unwilling to consider the possible failings in their product. Because attackers are always trying to discover new ways to break the security of tools, software and hardware often needs to be updated to fix new vulnerabilities. It can be a serious problem if the creators of a tool are unwilling to do this, either because they fear bad publicity or because they have not built the infrastructure to fix problems.

You cannot predict the future, but a good indicator of how software toolmakers will behave in the future is their past activity. If the tool's website lists previous issues and links to regular updates and information — like specifically how long it has been since the software was last updated — you can be more confident that they will continue to provide this service in the future.

When you buy a new device or a new operating system, keep current with its software updates. Updates will often fix security problems in older code that attacks can exploit. Older phones and operating systems are no longer supported, even for security updates.[35] What technology you use or buy today will become obsolete, and so will today's best advice about what software protects you and what surveillance technology has evolved to defeat them.

In the coming years, the last refuge of privacy and security in private encryption will come under attack. Law enforcement sentiments are rising in opposition to it as political candidates speak of a "surge"[36] in intelligence gathering and others encourage defeating public encryption with back doors, or by compelling duplicate plain text copies for every encrypted digital communication. England's former Prime Minister, David Cameron, once asked, "Are we going to allow a means of communications which it simply isn't possible (for governments) to read? My answer to that question is: No, we must not."[37] In a digital world bursting at its seams with hyper-invasive, aggressive surveillance, constitutional assurances of due process, effective assistance of counsel, and the attorney-client privilege will become hollow artifacts of a past American history unless criminal defense lawyers answer Cameron's question with "Yes, we must."

Notes

1. June 2, 2016, *Bloomberg Law* article by Gabe Friedman, quoting Edward Snowden: "Government surveillance is about power. These programs were never truly about terrorism, at least not solely. They were about power."

2. Five Eyes is a nickname given the five signees of a post-WWII treaty of joint cooperation in signals intelligence. Australia, Canada, New Zealand, the United Kingdom, and the United States share their surveillance output with each other, including the surveillance of each other's citizens.

3. Friedman, supra note 1, at 2; Dia Kayyali, Electronic Frontier Foundation, *Legal Community Disturbed About Recent Allegations of Spying on Privileged Communications*, Feb 22, 2014.

4. President Reagan issued Executive Order 12333 in 1981 and President Bush amended it in 2008 with EO13355. The NSA considers these orders as executive authorization for broad agency discretion in the implementation of the massive scope of its surveillance activities worldwide.

5. Section 4 of NSA's Section 702 minimization procedures, cited by Director Alexander in his 10/03/14 letter.

6. Alexander letter, supra note 5, at paragraph 9.

7. For more depth and context regarding these rule changes, see David Hudson, *NSA Surveillance Policies Raise Questions About the Viability of the Attorney-Client Privilege*, ABA Journal web article posted Sept. 1, 2014.

8. ABA Rule 1.6 Confidentiality of Information, paragraph (c).

9. Per the Model Rule 1.6's Comments at (18): "Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule."

10. Opinion 12-01 (February 2012), page 2, finding in sub-paragraph 1. Approved by the NACDL Board of Directors, February 19, 2012.

11. Quoting digest of NACDL Ethics Advisory Committee Opinion 02-01 (November 2002).

12. For an interesting read about the quandaries of self-protection from Internet surveillance, see Julia Angwin, Dragnet Nation (2014).

13. Aside from technological methods, the "social engineering" deceits of impersonation, of false representation of ties to defense personnel, and the infiltration of the defense team by private informants who befriend, entice, and emotionally or financially compromise defense staff, are separate risks no technology will protect against.

14. A Joint Task Force is a multi-jurisdictional operational intelligence gathering and investigative partnership drawing personnel from many federal and state law enforcement agencies that is charged solely with the investigation of one particular criminal activity or organization, such as terrorism, organized crime, drug cartels, or gangs.

15. Fusion Centers administer and promote information sharing between the CIA, FBI, the Department of Justice, the U.S. military, the private sector, and state and local law enforcement to provide investigative data for intelligence analysis.

16. Parallel construction is a strategy of deceptive omission or of false representation of facts used by law enforcement to conceal the true source of information used in a criminal investigation.

17. More information on diceware is available at https://ssd.eff.org/en/module/animated-overview-how-make-super-secure-password-using-dice.

18. The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. As part of its mission to promote privacy and security online, EFF has developed a website called Surveillance Self-Defense (https://ssd.eff.org), which includes detailed guides and how-tos on defending yourself from surveillance by using secure technology and developing careful practices. Much of the advice about software choices and secure computing was copied or adapted from the Surveillance Self-Defense guide, which is published under a Creative Commons Attribution license (i.e., is free for copying and sharing without prior permission).

19. A guide to using KeePassX is available at https://ssd.eff.org/en/module/how-use-keepassx.

20. To check and see if your system is encrypted, and to turn encryption on if it is off, follow the instructions at https://support.apple.com/en-us/HT204837. When your computer asks how you want to store your recovery key, choose the option that does not use your iCloud account, and then make sure to keep a physical (i.e., written-down) copy of your recovery key in a safe place. If you forget your password, you will need it in order to decrypt your computer.

21. For Windows 7 instructions, see https://technet.microsoft.com/en-us/library/dd835565.aspx. For Windows 8.1 instructions, see http://www.tomsitpro.com/articles/windows-8.1-the-missing-manual-book-excerpt,2-7234.html. For Windows 10 instructions, see http://www.groovypost.com/howto/use-bitlocker-encryption-windows-10/. In all cases, when you're given the option to save your recovery key, we recommend printing it out and then keeping a copy in a safe place. If you forget your password (or change your system's hardware), you'll need it in order to decrypt your computer.

22. For instructions on using DiskCryptor, see https://ssd.eff.org/en/module/how-encrypt-your-windows-device.

(Continued on page 63)

About the Authors

Sam Guiberson advises and assists other defense lawyers in cases involving undercover operations, recorded evidence, litigation technology, and other defense tactics and technologies of surveillance. He serves as Chair of NACDL's Technology Advisory Group.

Samuel Guiberson
Guiberson Consulting, PLC
713-520-7200
E-mail sam@guiberson.com
Web Site www.guiberson.com

Dr. Jeremy Gillula is a staff technologist at the Electronic Frontier Foundation, where he explains technology to lawyers (and occasionally the law to other technologists). He also serves as a member of NACDL's Technical Advisory Group.

Jeremy Gillula
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
415-436-9333
E-mail jeremy@eff.org

A Beginner's Guide to Surveillance, Digital Security, and the Privilege

(Continued from page 58)

23. To check if a device is encrypted, follow the instructions at https://ssd.eff.org/en/module/how-encrypt-your-iphone.

24. To find out if a device is encrypted, and to encrypt it if it is not, follow the instructions at http://www.howtogeek.com/141953/how-to-encrypt-your-android-phone-and-why-you-might-want-to/.

25. See endnote 17 for more information on choosing a strong passphrase.

26. Either way, make sure you are backing up your data!

27. Download HTTPS Everywhere from the Chrome Store, Mozilla Add-Ons website, or https://eff.org/https-everywhere/.

28. Privacy Badger can also be acquired from the Chrome Store, Mozilla Add-Ons website, or https://eff.org/pb.

29. A guide to using Tor Browser for Windows is available at https://ssd.eff.org/en/module/how-use-tor-windows. A guide to using Tor Browser for Mac OS X is available at https://ssd.eff.org/en/module/how-use-tor-mac-os-x.

30. Instructions for using Signal on iOS are available at https://ssd.eff.org/en/module/how-use-signal-ios, and on Android at https://ssd.eff.org/en/module/how-use-signal-android.

31. An introduction to PGP is available at https://ssd.eff.org/en/module/introduction-public-key-cryptography-and-pgp. A guide to using PGP on Mac OS X is available at https://ssd.eff.org/en/module/how-use-pgp-mac-os-x, and a guide for Windows is available athttps://ssd.eff.org/en/module/how-use-pgp-windows.

32. See endnote 17 for more information on choosing a strong passphrase.

33. 7-Zip is free, open source software, available from http://http://www.7-zip.org/.

34. Keka is free, open source software, available from http://www.kekaosx.com/en/.

35. In particular, Microsoft has made it clear that Windows XP and earlier Windows versions will not receive fixes for even severe security problems. If you use XP, you cannot expect it to be secure from attackers. The same is true for OS X before 10.7.5 or "Lion."

36. Dustin Volz, *Clinton Calls for U.S. 'Intelligence Surge' in Wake of Orlando Attack*, Reuters, Jun 14, 2016.

37. Nicholas Watt, Rowena Mason & Ian Traynor, *David Cameron Pledges Anti-Terror Law for Internet After Paris Attacks*, The Guardian, Jan. 12, 2015. ■

The Champion®

The Champion® (ISSN 0744-9488) is published monthly, except for January/February and September/October, which are bimonthly, by the National Association of Criminal Defense Lawyers™, Inc. Printed in the United States of America. Basic subscription rate $65 per year when received as a benefit of NACDL membership. Non-member subscriptions are $100 annually in the U.S. or $125 if mailed outside the U.S. Periodicals postage paid at Washington, DC and additional mailing offices. Postmaster: Send address changes to *The Champion*®, 1660 L Street, NW, 12th Floor, Washington, DC 20036.

The Champion® is published in the interest of the members of the National Association of Criminal Defense Lawyers™ to inform and educate the membership and to improve communication within the criminal defense community. See *www.nacdl.org* for details.

Statements and opinions expressed in *The Champion*® are those of the authors and are not necessarily those of the NACDL®. The information contained in The Champion® should not be construed as client-specific legal advice.

Publication of advertising does not imply endorsement. All advertising is subject to the approval of the Publisher. Advertiser and advertising agency assume liability for all content (including text, representation, and claims arising therefrom against the publisher).

Absent prior written agreement, material published in *The Champion*® remains the property of the NACDL®. No material, or parts thereof, may be reproduced or used out of context without prior approval of and proper credit to the magazine.