ONLINE PRIVACY FOR JOURNALISTS

A must-have guide for journalism in 2017

By **MICHAEL DAGAN**
Former Deputy Editor, Haaretz

Professional Advisor: **Ariel Hochstadt**
Security Expert, former Gmail Marketing Manager for Google.

TABLE OF CONTENTS

TABLE OF CONTENTS

01 INTRODUCTION

Many veteran journalists, but not only these, surely noticed that we are all of a sudden bombarded again from all-over with mentions of Watergate. Books like George Orwell's 1984 are on display at bookstores and an air of danger to freedom of speech and freedom of the press is spreading slowly like a dark cloud over the Western Hemisphere, raising old fears.

When an American serving president accuses a former president of surveillance; when he prevents central US media outlets access - so far always granted, and taken for granted - to press conferences he holds; and when he incessantly knocks and accuses the media of being the country's enemy number one, it isn't surprising that memories of President Nixon surface up more with every self-pitying tweet about SNL, and that even Republican Senators such as John McCain express fear for the future of democracy.

And McCain is not alone. Many journalists whom I have spoken with recently, expressed concern for whatever lays ahead for the freedom of the press. At a time when it's possible to express the following statement - "Donald Trump controls the NSA" - and not be held a liar, anything's possible. Add that to the fact that recent news on CIA taught us that almost all encryption systems can be compromised, if someone has the perseverance to crack them - and you are en route to envisioning an utterly Dystopian world, where you cannot even get too comfortable laying on your sofa, in front of your own smart TV.

The good news is that it is nevertheless possible to make it difficult for anyone to try and intercept your emails, the text messages you're sending or your phone calls.

You can take measures to make the lives of those who want to uncover your sources and the information being revealed to you, much harder. Of course, the degree of effort you're prepared to take to protect your privacy, your sources' anonymity and your data's safety, should be commensurate to the likelihood of a real threat, be that hacking or spying.

"The old-fashioned promises - I'm not going to reveal my source's identity or give up my notes - are kind of empty if you're not taking steps to protect your information digitally", says Barton Gellman of the Washington Post, whose source, former NSA contractor Edward Snowden, helped uncover the scope of the NSA's and British GCHQ's operations, to his interviewer Tony Loci. Loci herself, who covered American judicial system for AP, The Washington Post and USA Today, and was herself held in contempt of court for refusing to identify sources, would probably endorse that.

So, what is it that needs to be done to ensure that a journalist's sources and data are secure and well? Grosso modo, the tips can be described as falling within the following categories:

Isolating your devices and/or their environment - For example, the physical insulation of a computer for the purpose of checking files, or the use of prepaid mobile devices.

Securing on-device applications and functions – This is known as reducing the "attack surface", i.e. limiting the installed apps to the bare minimum, installing only from trusted sources, selecting apps that require minimal rights, keeping the system fully patched and updated, and having as many security controls (based on recent best-practices white papers) on the device.

Acting cautiously both in the digital and real world – This has a lot to do with common sense and a little less to do with software: For example, never write down the name of the source, certainly not on any app or on any document that's stored on your computer - and most certainly not on anything stored on the cloud.

02

COMMUNICATING WITH YOUR SOURCE AND SAFEGUARDING THE SENSITIVE DATA

Let's begin by listing what you can do when it comes to communicating with a source, and storing sensitive information obtained thereof:

1) Always encrypt everything: Security experts use simple math to make their point: as you raise the cost of decrypting your files (say, for intelligence agencies like the NSA), you automatically increase the degree of effort expended on following you. If you're not Chelsea Manning, Julian Assange, or Edward Snowden and if you weren't involved in active surveillance around Trump Tower apartments, They may give up the effort even if your encrypted communications were stored. And should anyone decide to track you despite your efforts, it will be more of a headache if you use strong encryption like AES (Advanced Encryption Standard) and tools like PGP or openVPN, which are the strongest widely available encryption methods (VPN's are used by the US government itself).
But if you want bullet-proof security, you will need more than the AES encryption method. P.S. if you want to discover the year your information landed at the NSA's hands, just have a peek here.

2) Perform full disk encryption: This is done just in case someone gets their hands on your computer or phone. Full disk encryption can be done using FileVault, VeraCrypt or BitLocker. Putting a computer to "Sleep" (instead of Shutdown or Hibernate) may allow an attacker to bypass this defense. Here, Mika Lee gives a complete guide for encrypting your laptop.

3) Beware of big names: Presume that large companies' encryption systems and possibly even big name operating systems (proprietary software) have back doors that secret services in their country of origin (at least in the US and the UK) can access. Bruce Shneyer, Security Expert, explains it here.

4) Avoid chatting with sources on the phone: All phone companies store data related to the

caller and the receiver's numbers, as well as the location of the devices at the time calls were made. In the US and several other countries, they're required by law to disclose information on registered calls in their possession.

What can be done? You should use a secure call service, such as the one the Signal app - which was tested repeatedly for security - possesses. Although this may mean that both the source and the editor need to download the app as well, the process takes just a few minutes. Here is a guide on how to use it. Just for the hang of it, check out how many of your non-journalist friends are hanging out there.

However you choose to communicate with your source, do not bring your mobile phone to sensitive meetings. Buy a disposable device and find a way to convey its number to the source in advance. The source needs to have a disposable safe device too. Authorities can track your movement through cellular network signals and it's advised to make it harder on them to locate you retroactively in the exact same cafe where the source was sitting. If you fail to follow this rule, all local authorities will be required to do is ask (politely and legally) for the video filmed by the café's security camera at the time of your meeting.

5) Choose secure messengers: your calls (cellular ones and via landlines) can be monitored by law enforcement agencies and each SMS is like a postcard - all text is fully visible to those who may intercept it. Therefore, use Messengers that allow for secure end to end call: signal, which was already mentioned above, and Telegram are considered to be the safest (although Telegram as well as WhatsApp's web apps were compromised once and then fixed).

According to some experts, you can also consider using SMSSecure, Threema and even Whatsapp.

The Signal Protocol has been actually implemented into WhatsApp, Facebook Messenger, and Google Allo, making conversations using them encrypted. However, unlike Signal and WhatsApp, Google Allo and Facebook Messenger do not encrypt by default, nor notify users that conversations are unencrypted - but offer end-to-end encryption in an optional mode. You should also keep in mind that Facebook messenger and WhatsApp are both owned by Facebook.

Adium and Pidgin are the most popular Mac and Windows instant messaging clients that support the OTR (Off the Record) encryption protocol and Tor – the web's best encrypted

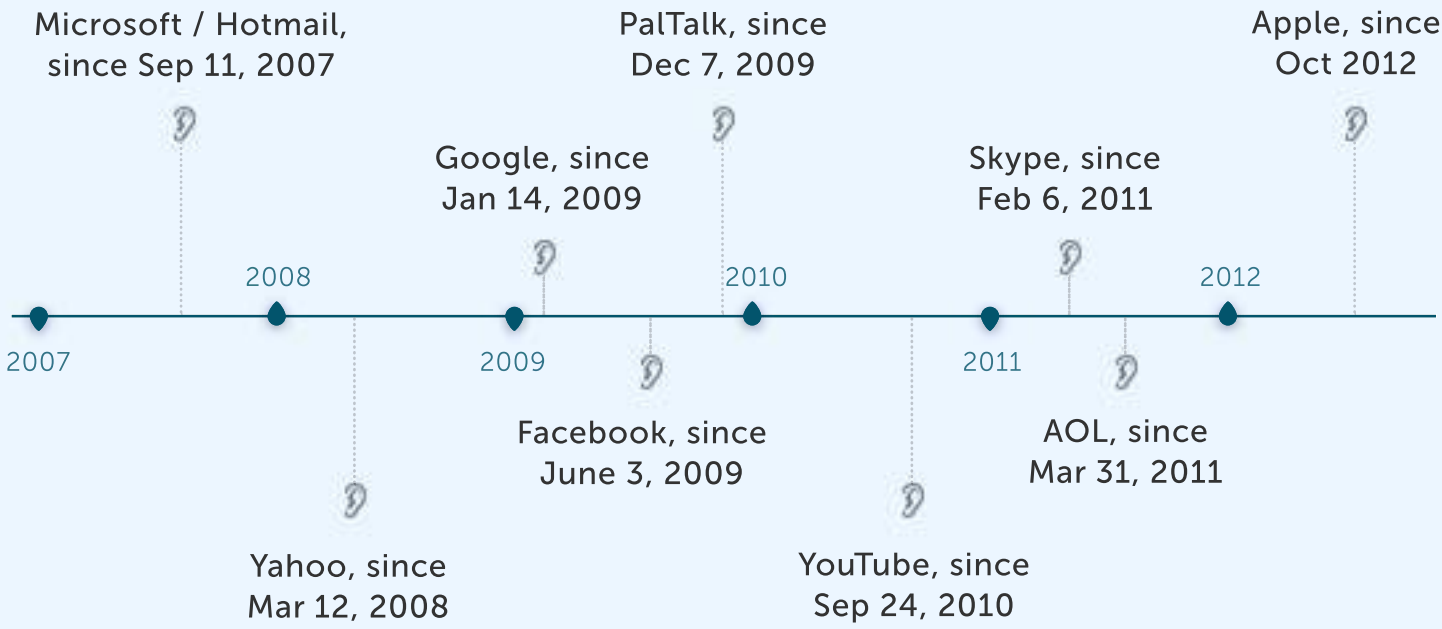
browser, which we will get to in detail later (See how to enable Tor in Adium here and in Pidgin here). Naturally, you could also use the Tor Messenger itself, which is probably the safest of them all.

Two final notes on texting: A cyber security expert I've discussed this with, says you should also have a working hypothesis that text is encrypted but the fact that these specific two individuals are talking, at this present time, might not go unnoticed.

The second note is you should also remember to delete the messages in your phone (although this may not be enough to withstand a forensic check), just in case your device falls in the wrong hands, to avoid exposing them.

How long is the NSA listening to you?

If you've been using email, video or voice chat, videos, photos, stored data, VoIP calls, file transfers or video conferencing, from any of the following services, then you are on e NSA database:



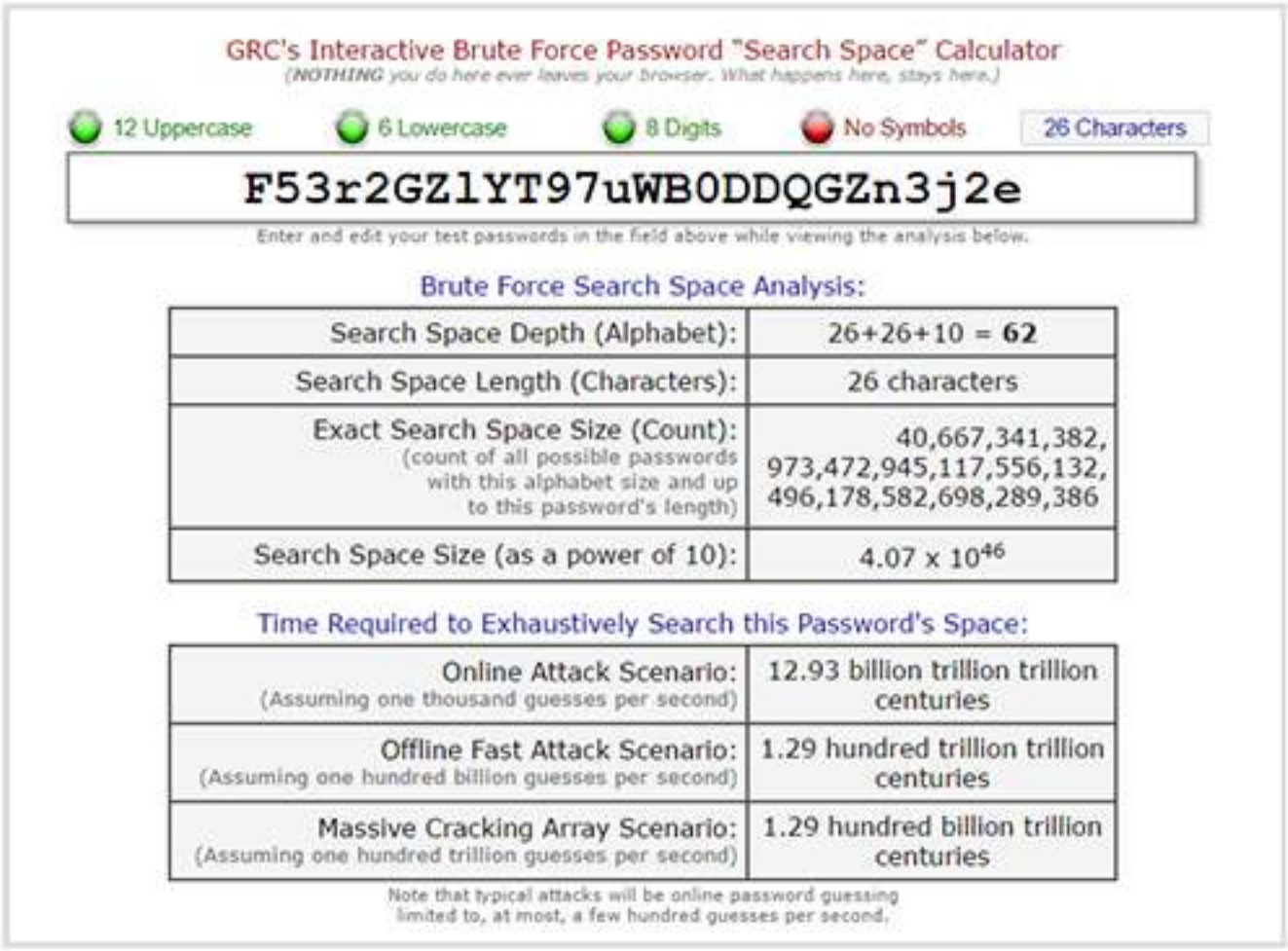
6) Do not use organizational chats: Slack, Campfire, Skype and Google Hangouts should not be used for private conversations. They are easy to break in, and are exposed to disclosure requests for courts use, to resolve legal issues at the workplace. Therefore, it's best to avoid them, not only when it comes to conversations with sources, but also conversations between colleagues, editors, etc., when you need to pass information received from your source, whose identity must be kept under cover. Many popular VoIP services like Jitsi have built-in chat features, and several of them are designed to offer most of Skype's features, which make them a great replacement.

7) In extreme cases, consider using a Blackphone. This phone, which strives to provide perfect protection for web surfing, calls, text messages and emails, is probably the best substitute for a regular phone if you are about to topple your government or getting ready to publish secret military files. An anti-bullet vest may also come in handy. Alternatively, try to do without a cell phone, Or opt for a cellular phone RFID signal-blocking bag. There's always an option that even the Blackphone can be tracked using its IMEI (the mobile phone's ID).

8) Protecting Data on your computer: It's very easy to break regular passwords, but it can take years to break passphrases – i.e., random combinations of words. We recommend trying secure password management tools like: LastPass and 1Password and KeePassX. You'll need to remember only one password, versus too many Passwords. And still, when handling important services such as your email, do not rely on password managers: Just make sure you remember the password.

In an interview to Alastair Reid in journalism.co.uk, Arjen Kamphuis, an information security expert, recommended that for encrypted hard drives, secure email, and unlocking laptops, one should choose a password of over 20 characters. Of course, the longer the password, the harder it is to crack - but the harder it is to remember too. That's why he recommends the use of a passphrase. "It can be anything, like a line of your favorite poetry," Kamphuis says, "maybe a line from something you wrote when you were nine that no one else will know about". Reid reports this thought provoking calculation, using the Gibson Research

Corporation's password strength calculator: A password like "F53r2GZlYT97uWB0DDQGZn3j2e", from a random password generator, seems very strong, and indeed it is, taking 1.29 hundred billion trillion centuries to exhaust all the combinations even when the software is making one hundred trillion guesses per second.



GRC's Interactive Brute Force Password "Search Space" Calculator

(NOTHING you do here ever leaves your browser. What happens here, stays here.)

12 Uppercase | 6 Lowercase | 8 Digits | No Symbols | 26 Characters

F53r2GZlYT97uWB0DDQGZn3j2e

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+26+10 = **62**
Search Space Length (Characters):	26 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	40,667,341,382, 973,472,945,117,556,132, 496,178,582,698,289,386
Search Space Size (as a power of 10):	4.07×10^{46}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	12.93 billion trillion trillion centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	1.29 hundred trillion trillion centuries
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	1.29 hundred billion trillion centuries

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

A 26 characters password...

The phrase: "I wandered lonely as a cloud", he points out, is so much easier to remember and is also more secure, taking the same software 1.24 hundred trillion centuries to exhaust all possibilities. Well, passphrase it will be.

GRC's Interactive Brute Force Password "Search Space" Calculator

(NOTHING you do here ever leaves your browser. What happens here, stays here.)

12 Uppercase | 6 Lowercase | 8 Digits | No Symbols | 26 Characters

i wandered lonely as a cloud

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+26+10 = **62**
Search Space Length (Characters):	26 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	40,667,341,382, 973,472,945,117,556,132, 496,178,582,698,289,386
Search Space Size (as a power of 10):	4.07×10^{46}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	12.93 billion trillion trillion centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	1.29 hundred trillion trillion centuries
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	1.29 hundred billion trillion centuries

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

...Is much weaker than a passphrase (screenshots from GRC.com)

9) Two-factor authentication is also a very good idea. In a regular two-stage authentication you sign in with your password and receive a second code, often via a text message to your smartphone. You can use Yubikey, as well as hardware tokens to further secure sensitive files on your computer. For more information, read the 7 golden rules for password security.

10) Assign a computer for inspecting suspicious files/attachments: The easiest way to distribute malware and spyware is through installation via USB or through attachments and email links. It is recommended therefore you use one air-gapped computer to examine these threats under quarantine. With this computer, you can freely use a USB and download files from the Internet, but do not transfer the files to your regular computer or re-use that USB.

11) How to buy your own secured computer: Security expert Arjen Kamphuis recommends purchasing a pre-2009 IBM ThinkPad X60 or X61. These are the only modern enough laptops with modern software systems, which enable replacing low level software. Another point to take into account is that you should not buy your computer online, as it may be intercepted during delivery. Kamphuis recommends buying it from a second-hand store for cash. He also points out that you should abolish all connectivity: Remove all Ethernet, modem, Wi-Fi or Bluetooth capabilities. Personally, I know security experts who wouldn't trust such a computer.

ThinkPad X60. Don't buy it online

12) Educating your Sources: It's possible that by the time the original and valuable information reaches you, it's already too late. Your source may have made every possible mistake, leaving behind a trail of evidence. But beyond the need to secure the information once it's in your hands, you should strive to teach your sources how to hide the information: store it securely and communicate safely via safe devices. Most people have no clue how to handle sensitive information, and in general what they're up against the moment they get in touch with you.

13) Use a designated secure system for receiving documents: Replace Dropbox or Google Drive and use something less popular but more secure. For example, SecureDrop is a designated system allowing you to receive files from anonymous sources and to safely scan and check them. Edward Snowden described Dropbox as "hostile to privacy" and recommended Spideroak instead. OnionShare is another free service that allows transferring files easily and anonymously.

How secure is cloud storage?

Most of the big providers of cloud storage - Amazon, Dropbox, Apple, Google, and Microsoft - have collaborated with the NSA at some point in the past. Most reserve the right to investigate all uploaded files, and will hand over the files to authorities when served a court order. There are still several things you can do about that:

1. Try to limit the number of files you upload to the cloud, and always encrypt them using strong encryption. The most secure and simple method is to manually encrypt the files, in which case you can use all Cloud storage services. Don't forget though: Do not upload your encryption keys to the cloud along with your files.

2. Use cloud services that automate encryption before uploading files, and sync everything with local versions. The provider might have the decryption key, but data risk is not as high as is the case with other Cloud providers. SpiderOak, which I've mentioned earlier, has apps for Android and iOS.

3. Cloudless Syncing with BitTorrent Sync - this it is not a true Cloud-based service, and cannot be used to store data for long periods of time, but BitTorrent Sync is free, and designed to be a replacement for Dropbox. All you need is to select the files, then you get a password and able to link that folder to another device's folder (if BitTorrent Sync is installed on it).

14) Don't keep notes – neither on a laptop, nor calendars or contact lists on your cellphone or computer or in the cloud - do not keep record of your sources name, initials, phone number, email or user name in messengers. Just don't.

15) Visual tracking: On the way to sensitive meetings, avoid using public transportation and guide your source to do the same. You should also avoid meeting places such as modern malls, where video cameras are spread all over the place.

16) Evading social media: Some people prefer to opt for radical anonymity. If for some reason, you need to vanish from the face of the earth without leaving a fully blown profile behind on every social media, totally delete your accounts. It's different from 'deactivating' them, a state in which all your info is stored and can be re-activated.

17) Make friends among hackers: This will help you avoid big mistakes, save time and headaches and keep you up to date on the technological arms race.

18) Payment method: Pay for everything in cash, consider using Bitcoins - buy them anonymously (use this Business Insider guide for that purpose) – and, if you have somebody willing to accept them at the other end of the transaction, use Darkcoin. A pre-paid credit card from an online store is also an option.

19) Scribble wisely: If you jotted down information on a piece of paper, what they used to call a note in the Precambrian world, destroy it. And don't forget even that wrinkled one at the bottom

03 HOW TO BECOME ANONYMOUS ONLINE

Beyond securing the communications with your source, and protecting possible breaches of the sensitive data you get hold of, you should also avoid being tracked while browsing. Online habits can disclose or provide hints as to the story you're working on, or worse, hint or disclose the identity of your source. Here are the golden rules for surfing the net safely and then, at the next chapter, for securing your email account:

1) Private browsing mode: There are two basic ways to maintain anonymity while surfing the web. The first, most basic and popular, yet insufficient way is to browse the information in private mode, an option that most browsers allow. Your browsing history will not be saved, and basic tracking technologies, which advertisers use, such as HTTP cookies, will be prevented from creating your detailed profile. But this is more of a nice to have privacy: It basically hides your browsing history from family members who can access your computer. Your IP address can still be monitored and information regarding all the sites you visited is still exposed to your ISP.

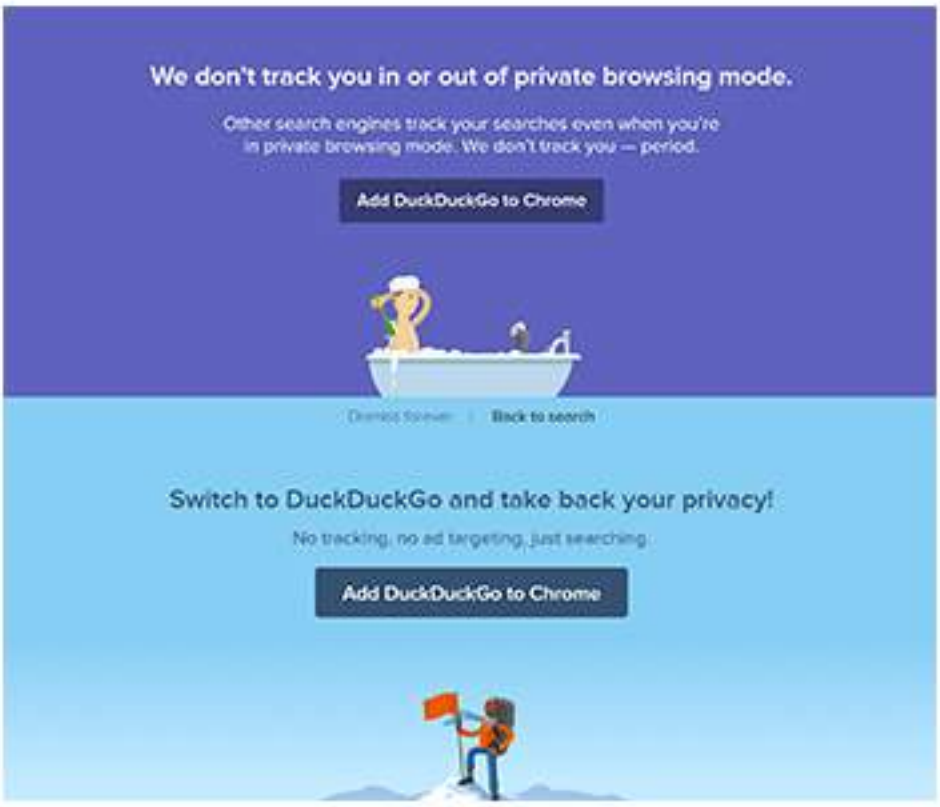
2) Use alternative browsers: browsers, such as Dooble, Comodo Dragon or SRWare Iron, which focus on user privacy, are limited in capabilities. You can achieve a similar degree of privacy offered by these browsers simply by deleting cookies - bits of code which have been downloaded to your system by websites you visit, that monitor your activity and sometimes even follow which content you consume; Another way to remain anonymous is by neutralizing your browser's location settings, and installing various features aimed at achieving anonymity. To check whether you disabled all cookies effectively, you can use the app CCleaner, which also handles Flash cookies, but none of these browsers are fully encrypted. The only standard browser that ensures total privacy is the Tor browser. Tor is ugly and slow, but it will protect you and your sources. The next section will give a more detailed account of it.

3) TOR: This "notorious" browser, which was developed by the US Navy, allows you to operate in a hidden network, carry out private communications and set up web sites anonymously. Tor's browser, which can be downloaded at Torproject.org, makes it very difficult to monitor your activities on the internet, or let governments or your ISP pinpoint your location. The only drawback is that it's slow at times,, a bit cumbersome - but that's only

because Tor routes you through three encrypted random relays around the world, before landing you at your destination site. You should also bear in mind that your neighbors may be shady characters.

Another option related to Tor is to download Whonix, a secure operating system that is focused on privacy. It works as an access gate to Tor, and only allows connections with Tor sites and users. But the most popular Tor OS is Tails (The Amnesiac Incognito Live System). Tails can be booted from a USB stick or DVD, and it anonymizes all information. Edward Snowden is considered a fan of this software. Qubes is another OS that supports Whonix and is recommended by Snowden.

4) Alternative search engines: Google, the most popular search engine, saves your search history in order to optimize the results. To stop this personalization you should click on: Search Tools > All Results > Verbatim. Or you sign into your Google account on www.google.com/history, find a list of your previous searches and select the items you want to remove by clicking the 'Remove Items' button.



DuckDuckGo. A search engine that doesn't store your info

But to avoid being monitored entirely, it's preferable to use a search engine such as DuckDuckGo. If you find it difficult to give up Google, download Searchlinkfix to at least keep away URL Trackers.

5) Direct treatment of "short-term" computer memory: Another way to neutralize options for monitoring your surfing is by deleting the DNS (domain name system) cache. Deletion is done using simple commands in the operating system. Rebooting the router – which sometimes has a DNS cache - or rebooting the computer can also reboot both their respective DNS cache, if the router has one.

6) Try to avoid HTML Web Storage - Web Storage is built into HTML5, and unlike cookies, the stored information is impossible to monitor or selectively remove. Web storage is enabled by default, so if you're using Internet Explorer or Firefox, simply turn it off. You can also use the add-on Better Privacy for Firefox to remove the stored information automatically. The Click and Clean extension will do the same job for Google Chrome.

7) Use a VPN: As I mentioned already, your ISP can monitor the sites you surf, and anyone who wants to eavesdrop on you, can also intercept your communications. To protect all incoming and outgoing communications, it’s important to make use of a VPN (For a complete explanation, click here). VPN encrypts all your communications, so that even the ISP or the secret services, or just hackers hovering around your favorite coffee shop’s Wi-Fi, won’t be able to know who you sent an email to, which service you used, etc.

The use of a VPN is very common among people who, for example, wish to see the complete Netflix movies catalog outside of the United States, but not every VPN is suitable for journalists. A VPN for journalists won’t necessarily be the fastest one or have the best support, but it has to be trusted not to keep VPN logs - that is, it cannot determine who you are, what sites you’ve visited and so on.

A safe VPN is bound to be provided by a company who’s not located at one of the "14 Eyes" countries, where intelligence networks are allowed to collect and share information with one another; firstly and foremost, in the USA. So VPN companies located in the territory of the former Soviet Union countries have an advantage. Their courts do not easily hand out orders

to retrieve information collected by local companies, be it regarding their citizens or foreign nationals. Here you'll find a list of 5 VPN services that stand out regarding privacy and all are located outside the "14 Eyes" countries.

By the way, even if governments are out on the hunt for Traffic that is sheltered by a VPN, you can still use stealth VPNs like TorGuard, to confront the challenge, whether it is active government censorship or just spying you're dealing with. Tor and VPN's give you the perfect protection when someone is trying to retrieve your browsing history in order to profile you.

Some tips from Edward Snowden

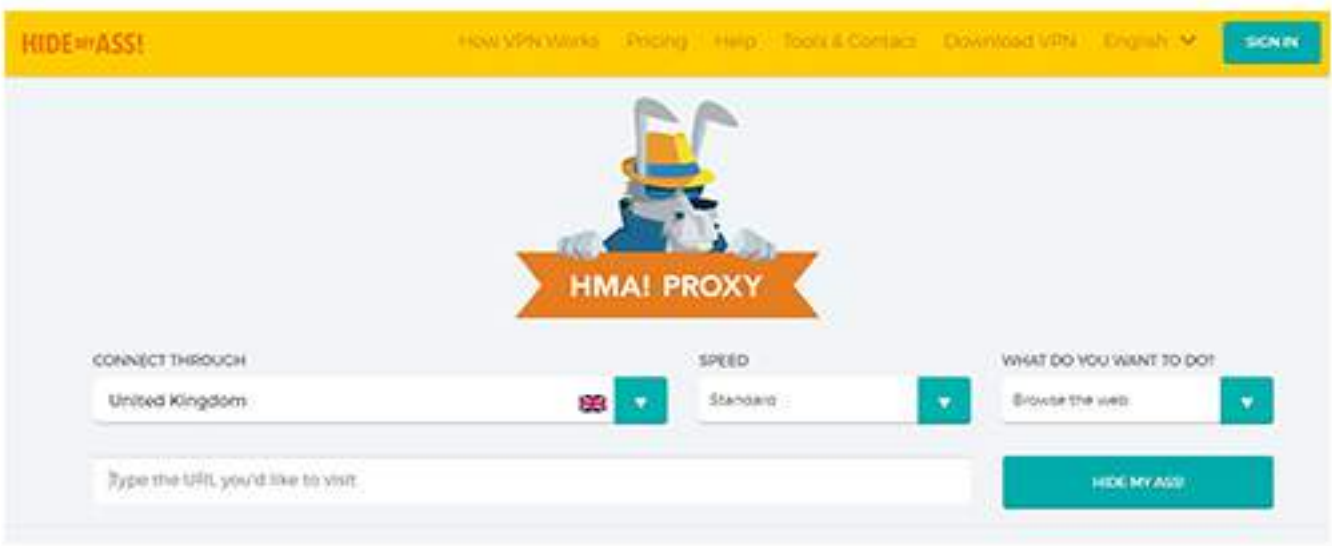
Adapted from an interview to Micah Lee on the Intercept

1. Encrypt your phone calls and text messages. You can do that with Signal, which is easy to use.
2. Encrypt your hard disk, so that if your computer is stolen, the information isn't retrievable.
3. Use a password manager. One of the main things that gets people's private information exposed are data dumps. Your credentials may be revealed because some service you stopped using in 2007 gets hacked, and the password also works for your Gmail account. A password manager allows you to create unique passwords for every site that are unbreakable, but you don't have the burden of memorizing them.
4. Use two-factor authentication, so if someone does steal your password, it allows the provider to send you a secondary means of authentication.
5. In every step, you have to stop and think, "What would be the impact if my adversary were aware of my actions?" If the answer is making you nervous, change or refrain from that activity, and try to mitigate that through some tools or system to protect the information and reduce the risk, or ultimately, accept the risk of discovery and plan your response. You can't always keep something secret, but you can definitely plan your response.
6. Selective sharing - don't spray your personal info everywhere.
7. Use ad blockers. Service providers are serving ads with active content that can be a vector for attack in your web browser — you should be actively trying to block these.
8. And finally, a quick guide for the whistleblower:
a. Tell no one who doesn't need to know about the wrongdoing you've uncovered.

b. Use something like SecureDrop, over the Tor network. People in a repressive regime should also always use Tor
c. Use a non-persistent operating system like Tails
d. Use a disposable machine that you can get rid of.
e. In other words - leave no trace. The only outcome of your operational activities should be the stories reported by the journalists.

8) Repair DNS leaks: Using a VPN does not protect you completely, because that DNS Traffic may hint at your identity. DNSLeakTest.com will allow you to detect such leakage. If the test shows that DNS is of your VPN, you can relax, but if it shows that the DNS is of your ISP, you are not anonymized. In this case you, check out what you can do here.

9) Virtual Machines. This nifty little trick is actually a second (virtual) computer, which operates as an app in your operating system. You can download files or open links in a similar way to the isolated computer I recommended earlier, so that your computer is less exposed to malware or spyware of any kind. Virtualization software, like VirtualBox should be opened using a secure operating system. File downloading is done with the virtual machine Internet connection shut down; after using the file, you'll need to delete it - and depending on your adversary, perhaps delete it along with the machine.



HideMyAss proxy server. I'll hide yours, if you'll hide mine

10) Proxy server: As in the case of virtual machines, here too the activity moves to another “area” and allows you to keep safe from spying and other attacks. Actually, the proxy servers substitute your IP address with theirs, which can mislead people into thinking you’re in a different country, for instance. HideMyAss.com/proxy, Psiphon (open source) and JonDonym all provide a similar service. Some experts say that these should be used with a VPN and/or Tor for higher levels of security. But then, some experts I’ve talked to claim that if you bother using Tor, you’re as secured as one can be anyway.

11) Three more types of extensions that can increase your level of security: To verify that the Internet protocol where you operate is https secure, you can install an extension called HTTPS Everywhere , made by the Electronic Frontier Foundation's (EFF), one of the organizations that funds the Tor Project. This extension is recommended by many cyber experts; it will ensure that websites you visit use the secure protocol, which is definitely not an insurance policy against anything, but better than the unencrypted protocol.
The second type of extension controls the data that javaScript is revealing to websites (in order to improve your browsing experience). Two popular options here are ScriptSafe and NoScript.

Another extension is the Ghostery browser. This extension will reveal who is following you among 2,000 companies, and will allow you to block unwanted ones. It’s sweet, but you probably won't be blocking the NSA this way. Privacy badger, a project by the EFF, also works similarly.

Anti-Malware, Antivirus and Firewall Software

Anti-Malware - There is a massive amount of malicious code, known as Malware, on the internet. Bitdefender comes installed on all versions of Windows newer than Vista. There are also Malwarebytes and Spybot Search and Destroy, that are both free.

Antivirus - After buying a new computer or a clean install of an operating system, this should be the first program you will install. Viruses can not only mess up your computer, but help

steal all information processed through it. Most people do have antivirus software installed on their computers, but not on their smartphones. Phones with open-source systems, such as Android phones, are more susceptible than those with closed-source systems, such as iOS (Apple) phones, to mobile viruses.

Firewall - A firewall ensures that no software is accessing your computer. Their drawback is that they have a hard time determining which programs are safe.

04 SECURING YOUR EMAIL

How should you protect your e-mail? The problem with maintaining the confidentiality of emails is even tougher: Google and Microsoft will most likely just give out your emails to government agencies if and when required to do so. What should you do?

1) Safe extensions: The simplest option, assuming you use common Web mail services such as Yahoo and Google, is to install the browser plugin Mailvelope, and make sure that the person on the receiving end does too. This extension simply encrypts (and decrypts) the e-mail. A similar but limited extension to Gmail called SecureGmail will perform a similar job. Emails that go through this extension are encrypted, and can't be decrypted by Google. Another possibility is "Encrypted Communication", which is a simple to use Firefox extension. For that you will need a password that the recipient has access to - but remember to never transmit the password by email.

2) Secure email providers: Hushmail is an example of an email service that provides better security than the more common networks you use, but it may be forced to hand over emails to the US government under a court order, and it does log IP addresses. Another email service with similar features and security levels is Kolab Now, which prides itself amongst other things with storing data exclusively in Switzerland.

3) Disposable Email Addresses (DEA's): This is an email created ad hoc for a specific purpose, which is completely anonymous and is deleted immediately after use. This solution, commonly used when signing up for various services in order to avoid spam, is also a great solution for maintaining anonymity. However I wouldn't advise journalists to communicate with their sources over it, because security is not its strongest trait. There are dozens of such temporary emails, but the British Guardian, for example, recommended Guerrilla Mail and Mailinator.

Using Guerrilla Mail in the Tor Browser ensures that not even they can connect your IP with your email address. Likewise, if you use email encryption software, such as GnuPG, on Tor, you're all set and secure. So, let's talk a bit about email encryption.

4) Encrypting your mail: Wired got this recommendation from Micah Lee, a privacy-focused technologist who worked with the EFF and First Look Media (here is an interview Lee held with Edward Snowden): Encrypting messages with webmail can be tough. It often requires the user to copy and paste messages into text windows and then use PGP to scramble and unscramble them (PGP - Pretty Good Privacy - is an encryption program that provides cryptographic privacy and authentication for data communication). That is why Lee suggests a different email setup, using a privacy-focused email host like Riseup.net, the Mozilla email app Thunderbird, the encryption plugin Enigmail, and another plugin called TorBirdy that routes its messages through Tor.
As Reid pointed out in his interview with Kamphuis on journalism.co.uk, Greenwald almost lost the NSA story because he initially ignored Snowden's instructions on email encryption. In other words, if you want a story that will go down in history it makes sense to be secure.
Kamphuis agrees that PGP can be trusted. As he and Reid explain, with PGP encryption, you have a public key, like your public phone number, and a private key. The public key can go on Twitter biographies, business cards, websites and wherever else your work is publicized, but the private key must be stored securely, as with any other sensitive information. Then, when a source wants to send information, they will use your public key to encrypt their email, that only your private key can unlock.
Kamphuis recommended the GNU Privacy Guard, an open-source version of PGP, that is simple to set up and has an active support community. For encrypting files, data and hard drives, he suggested consulting his freee eBook, “Information security for journalists”, published with Silkie Carlo and released through the CIJ, which fully explains the process.
If you do choose to encrypt the message itself regardless of your mail provider’s identity, using zip with a password is a good idea, and 7ZIP is a recommended tool for accomplishing that.

5) Back to basics: Yes, I know that this is back to email security 101 - but please try to avoid phishing. Watch the “from” field in your email for little misspellings; someone else can pose as somebody you know.
And one last word on email encryption: One of the real problems to bear in mind is that even after encrypting them, not everything is encrypted. The email addresses of the sender and recipient, the subject line and the time and date when the email was sent, are all out on the open. Attachments and the message itself are the only data that is encrypted.

A case study: The Rosen affair

The James Rosen affair is worthy of special attention. That is not only because the FBI convinced a court to treat a senior journalist (Fox News chief correspondent in Washington, D.C) as a suspect in an espionage case - labeling him a criminal co-conspirator - for routine steps a reporter takes when working a source in the corridors of power. It is worth noting, mainly because it highlights flaws in reporting techniques, and it once again raises the question whether reporters and media organizations are doing enough to protect sources.
As the Guardian's Glenn Greenwald reported, The FBI tracked Rosen's movements in and out of the State Department, traced the timing of his calls, and even obtained a search warrant to read two days' worth of his emails, as well as all of his emails with his source, Stephen Jin-Woo Kim.
Tony Loci writes in an article titled "Surveillance and Security" that "Rosen and Kim spoke on landlines and cellphones inside the State Department: The reporter used a pressroom line and Kim used his office phone. Kim reviewed a document about North Korea on a classified computer, while on the phone with Rosen. The latter set up an unsecure e-mail account to communicate with him.
"The FBI's affidavit says they lined up the phone numbers, compared the calls' timing to log-ins at Kim's secret computer, cracked nicknames they used as code in email, and tracked the State Department security badges they swiped when they left and returned to the building within minutes of each other". As terrifying as the Trump administration might seem now, it is still worth reminding again the astounding fact that under Obama, the justice department has prosecuted more government leakers under the 1917 Espionage Act than all prior administrations combined - in fact, double the number of all such prior prosecutions. It is true that Kim, a naturalized citizen from South Korea, was indicted in 2009 for allegedly telling Rosen that US intelligence believed North Korea would respond to additional UN sanctions with more nuclear tests - but as Fox news contributor, Judge Andrew Napolitano, put it well: "This is the first time that the federal government has moved to this level of taking ordinary, reasonable, traditional, lawful reporter skills and claiming they constitute criminal behavior". Greenwald gets to the same conclusion in theguardian: "...the DOJ specifically argued that by encouraging his source to disclose classified information - something investigative journalists do every day - Rosen broke the law". Greenwald calls this "criminalizing the act of investigative journalism itself"' and points to the fact that this trend has actually started back when the New York Times reported in 2011 that "Obama's DOJ has been using that same 'solicitation' theory to justify its ongoing criminal investigation of WikiLeaks and Julian Assange: that because Assange solicited or encouraged Manning to leak classified information, the US government can 'charge [Assange] as a conspirator in the leak, not just as a passive recipient of the documents who then published them.'"

05 FINAL WORDS

These are perhaps the most radical pieces of advice I ran through, when preparing this eBook.

As Micah Lee put it when interviewed on privacy on WIRED: “If your computer gets hacked, the game is over. Creating a virtual sandbox around your online communications is a good way to keep the rest of your system protected. Tor is awesome and can make you anonymous. But if your endpoint gets compromised, your anonymity is compromised too. If you really need to be anonymous, you also need to be really secure”.

And Journalist Tony Loci puts it in even harsher words in an article published in an eBook about the future of cross border investigative journalism for the Nieman foundation at Harvard: “Some journalists, computer scientists and privacy advocates are so alarmed that they recommend reporters go old school... and rely on in-person interviews and snail mail”.

I hope I have helped people in the trade, and others, gather some information that will clarify what needs and can be done to ensure your and your source’s security in these hectic times.

06

LIST OF SOURCES FOR THIS E-BOOK

Security for journalists: How to keep your sources and your information safe
http://www.ire.org/blog/car-conference-blog/2016/03/12/security-journalists-how-keep-your-sources-and-you/

Securing data, sources and yourself
http://www.ire.org/blog/car-conference-blog/2017/03/05/securing-data-sources-and-yourself/

Surveillance and Security: Are reporters and news organizations doing enough to protect sources?
http://niemanreports.org/articles/surveillance-and-security/

Muckraking Goes Global: The Future of Cross-Border Investigative Journalism
http://niemanreports.org/books/muckraking-goes-global-the-future-of-cross-border-investigative-journalism/

The Ultimate Guide for Online Privacy
https://www.vpnmentor.com/blog/ultimate-guide-online-privacy/

What Is a DNS Cache?
https://www.lifewire.com/what-is-a-dns-cache-817514

How to Anonymize Everything You Do Online
https://www.wired.com/2014/06/be-anonymous-online/

19 ways to stay anonymous and protect your online privacy
https://www.extremetech.com/internet/180485-the-ultimate-guide-to-staying-anonymous-and-protecting-your-privacy-online

Edward Snowden explains how to reclaim your privacy
https://theintercept.com/2015/11/12/edward-snowden-explains-how-to-reclaim-your-privacy/

LIST OF SOURCES FOR THIS EBOOK

Information security for journalists: staying secure online
https://www.journalism.co.uk/news/information-security-for-journalists-/s2/a562525/

NSA targets the privacy-conscious
http://files.gendo.nl/presentaties/CIJ_Infosec&countersurv_4-07-2014.pdf

Obama DOJ formally accuses journalist in leak case of committing crimes
https://www.theguardian.com/commentisfree/2013/may/20/obama-doj-james-rosen-criminality

Your WhatsApp secrets are safe now. But Big Brother is still watching you…
https://www.theguardian.com/commentisfree/2016/apr/10/whatsapp-encryption-billion-users-data-security

Obama Pursuing Leakers Sends Warning to Whistle-Blowers
http://www.bloomberg.com/news/2012-10-18/obama-pursuing-leakers-sends-warning-to-whistle-blowers.html

6 encryption mistakes that lead to data breaches
https://www.crypteron.com/blog/the-real-problem-with-encryption/?gclid=Cj0KEQiA9P7FBRCtoO33_LGUtPQBEiQAU_tBgDgBzD9wIXv94vwhj3qwhc6ewEYYeyjIeiXtMQiwF3caAsFn8P8HAQ

ABOUT THE AUTHOR

Michael Dagan is currently transitioning to content strategy and content marketing for startups, after some 25 years in senior editing positions in Haaretz group, the leading Israeli media. In his last role, he was deputy editor of Haaretz, overseeing and coordinating all operations: print, digital and Hebrew & English editions, as well as related activity such as conventions.

Dagan is a seasoned magazine editor who oversaw many investigative reporting endeavors over the years, both as Haaretz' weekend magazine chief editor, and as the chief editor of Haaretz' economic monthly - TheMarker magazine - which under his supervision was the leading magazine in the country. Dagan also conducted many of Haaretz' innovations around the weekend edition - which is one of Haaretz' main growth engines today - amongst others, the launching of an iPad edition for Haaretz magazine. He's not paranoid, and still on social media: @mikedagan on twitter, and Michael Dagan on Linkedin.