THE DEATH OF SOURCE PROTECTION?

Protecting journalists' sources in a post-Snowden age

By Carl Fridh Kleberg

Polis/ Journalistfonden Fellow

Table of contents:

1. Executive Summary

- The revelations of mass surveillance by Edward Snowden have highlighted the potential threat to the privacy of journalists' communication and data, calling into question the ability to protect anonymous sources.
- Threats to the privacy of journalists can come from a number of sources including government agencies, employers and service providers.
- There are a number of tools available to help maintain privacy of communication but using these can sometimes draw unwanted attention in themselves and there is no tool that is 100% safe.
- There is a need for training and awareness-raising amongst journalists, and media organisations will expect the next generation of journalists to be more 'data savvy' - something that is not yet the case.
- There are a number of simple steps you can take to increase data security such as continuous 'password hygine' and an awareness of privacy and location settings on devices like mobile phones.
- When assessing risk to a source, journalists need to be aware of the compromising potential of electronic communications and may need to go 'offline' for the most risky of cases.

2. Introduction

It was a major scoop by any standard, but the Edward Snowden revelations also sent a chill down the spines of journalists. They confirmed what many already suspected. The scope of mass surveillance and the extent of the authorities' power is especially troubling for a profession that places uncompromising source protection above most, if not all, other professional virtues. More worrying, journalists as a group often combine concentration of sensitive information with a less than perfect grasp of technical know-how.

Journalists are forced to consider what protection they can guarantee their sources. The conclusions some draw are dismaying. Can any technology be trusted, when hardware and software appear as leaky as sieves? Can any legal guarantees be relied upon, when decisions are made in obscure systems with scant transparency, where even privileged communications between lawyers and clients are subject to eavesdropping? Even journalists that recognise a government need for law enforcement and intelligence are worried.

It all boils down to a single worrying question: is source protection dead? While the answer may be 'no', even an optimist would deny that there is a new and significant threat.

But while many have described initial reactions of shock and confusion, some attempts to tackle these concerns have followed. While the Snowden revelations shed light on the extent of snooping, they also suggest there are tools that offer some degree of protection. Using relatively simple steps, journalists can vastly improve their ability to protect information, and journalists are expanding their toolboxes with these skills.

Yet absolute promises of security should be met with some suspicion, and some journalists interviewed for this report describe abandoning digital communications altogether in the most sensitive of cases. There are also concerns that the discussion has become too technically advanced, or that it focuses solely on solutions with state surveillance in mind when few journalists will face so advanced an adversary.

The goal of this report is to offer a very basic introduction to some of the main digital security challenges faced by journalists today, such as eavesdropping on wired communications, protection of data stored on drives, and email communications. We also seek to introduce attempts to tackle these issues, such as training, software, legal challenges, or even "going old school".

It's aimed at journalists or others seeking a basic inroad into the subject and we hope it will be of some interest to those more experienced in the field. It will draw on real-life examples relevant not only to those pursuing global scoops on the Wikileaks level, but also more routine reporting on crime, employment and social issues.

We hope it will prove both interesting and useful, serve as one first step on the road towards a strengthened source protection, and offer some guidance in where to proceed from there. Please let us have your feedback via Polis@lse.ac.uk .

3. What are we looking at?

3.1 Identifying threats and assessing risks

The first question to anyone trying to figure out how to make their communications more secure is: Against what?[1] It's easy to get caught up in reasoning about how to protect your data from state intelligence agencies, when the biggest threat many sources face will be their employer, their colleagues, or social acquaintances.

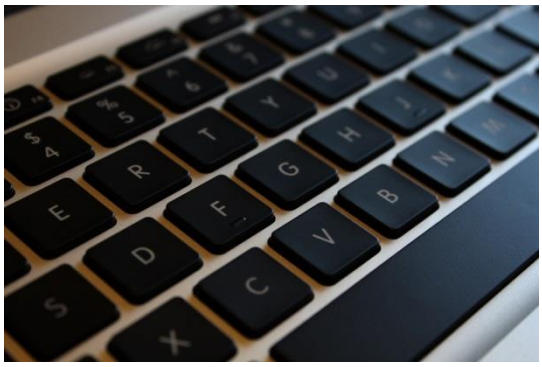
Many of the risks journalists need to consider are less about what the NSA or GCHQ know and more about what people around the source can glean, what overly talkative network administrators can read in your emails, what Internet Service Providers (ISP) record, and what the owner of that site you visited 20 times a day under the course of your investigation can tell from those visits.

While the issue of state level surveillance needs to be taken into consideration and the responsibility to protect sources is wide in scope, consider what the most pressing risks you face are. While heavily encrypted email and data traffic may be necessary, it may be more urgent to tackle basic mistakes

[1] Anyone investigating this subject might encounter the term Operations Security or "OPSEC" which has made its way from military terminology into privacy lingo. An associated term is Information Security or "INFOSEC". In short, OPSEC is the process of assessing threat and possible counter-measures in a wide sense that goes beyond data protection (which would usually fall under INFOSEC). While the Tinker Tailor Soldier Spy-lingo may seem a bit tiresome at times, but it's worth considering the difference between the two and what they mean for journalists.

such as communicating sensitive information via work phones or computers, storing unencrypted sensitive information online, sloppy password management, or publishing photos with embedded location data.

For instance, few prying employers are likely be able to pressure companies like Google or Facebook into handing over conversations, or force the company that built your mobile phone to grant access to your stored data. Law enforcement agencies on the other hand can do just that. Advanced encryption may protect the contents of your communications but also set off warning bells that draw attention. Driving around in a black SUV car without number plates will obscure what's inside, but will likely be perceived as more than a bit suspicious. On the other hand, unencrypted data is normally easy to eavesdrop on and even more common encryption that will not alert an eavesdropper might be easy to break.



One problem with assessing the threats you face is the fact that the capabilities of the authorities and other organisations are often unknown. What Snowden made public was information on capabilities up to a point in time, not necessarily what is possible today. Another point is that data can easily be stored for an indefinite time and it is difficult to know what information might become compromising in the future. For this reason a policy of "better safe than sorry" is advisable, and it is important to understand that really protecting a source may well mean going above and beyond the most pressing threat.

Frank Smyth, executive director of the firm Global Journalist Security and senior advisor for journalist security at Committee to Protect Journalists, emphasises that journalists need to consider first and foremost what they're up against. In some cases, simply dividing communication between different accounts and services will make a big difference in how difficult tracking communications will be.

> *"It depends on your profile and that's why you want different ways of communicating. It's about always keeping it in a variety of places so nobody can get it all, unless they're devoting a whole room full of people to look at you," he says. "That's the way to stay safe, I think. Basic operational security online."*

Smyth believes that at times the discussion is too focused on advanced tools and strategies with adversaries like the NSA or CIA in mind. For some people it is a relevant threat level to consider, but not for everyone, he says. For instance, he advises strongly against actively using PGP or TOR to encrypt every file or email saying that he first of all does not know if any technology is trustworthy, and adding that such an approach would be adapting to a threat level far higher than necessary. He compares that with teaching every single person dentistry rather than basic dental hygiene:

> *"I teach people basic things – how to brush and floss their teeth. They need to know the risks to make choices. You start going into some tools and it just confuses people."*

Thinking carefully about what risks you face is key to working out how to communicate more securely. Different people may then draw different conclusions (some, for instance, will recommend encrypting as much as possible to make specific data less suspicious while others will advise some degree of hiding in plain sight) but it is important to do the research and have the discussion.

3.2 Legal and policy challenges

Source protection, source confidentiality, reporter's privilege – there are many different labels used to describe the phenomena. Today the onus on journalists to protect the identity or other information about their sources is a well-established principle in many parts of the world. For many journalists, few professional sins rank more grave than to expose, or fail to protect, a source. In Sweden where source protection is enshrined in the constitution, failure to protect an anonymous source can land a journalist in prison.

Few countries offer this level of legal protection for the sources of journalists, but in many places there is some protection in theory at least. In the United States there are varying shield laws depending on the state in question. In Europe, the European Court of Humans Rights has ruled that the protection of journalists' sources is a basic condition for press freedom.

At the same time, source protection as a principle has regularly clashed with other interests of both public and private actors. There have, for instance, been numerous examples of eavesdropping on journalists and their sources in European countries despite the rulings of the ECHR, and the perceived sanctity of source protection has been questioned both in connection to law enforcement and intelligence gathering. The current United States government has been described as unusually aggressive in pursuing leaks from within the administration.

Revelations of mass surveillance and other telecommunication eavesdropping have called into question to what degree source protection can be guaranteed, and some journalists argue that surveillance effectively makes source protection impossible. This in turn has led to multiple new legal challenges with policy change as an aim, in the hope that the conflict between the protection of sensitive communication and mass surveillance will lead to limitations on the latter.

There are many on the technical and privacy activism side who express scepticism that legal and policy reform will have any effect, pointing to cases where laws governing privileged communications between lawyers and their clients in the UK have failed to deter surveillance by law enforcement. With this in mind, the legal perspective on source protection online and what the legal consequences of surveillance or weak data security are will *not* be the focus of this report.

3.3 On the wire

What we do on the internet is continuously monitored not only by authorities for surveillance purposes. It is done by Internet Service Providers (ISPs), company IT desks, companies providing the sites and services we access online, and many others. All unprotected traffic through a network can be monitored by its administrators, or anyone who can get similar access including authorities or

criminals. Furthermore, internet traffic does not only travel from point A to point B, but rather skips around servers all over the world each with separate administrators.

An unencrypted email or file sent through a network is no safer than a postcard in the mail and can be read by anyone monitoring that network. This includes data leaving VPN or TOR networks (described further below). Data can also be saved indefinitely, which is important as it's not always clear what might be deemed sensitive in the future. And beyond the actual contents of a message being visible, there is also "metadata" – information about the message such as sender and recipient, which may in itself be damning enough.

One way of protecting your traffic is encryption. Edward Snowden has said that encryption works, and that properly implemented strong crypto systems "are one of the few things that you can rely on". While proper implementation is a significant undertaking, this at least suggests that data protection is possible, one of the few things in the Snowden revelations that the security-minded have found encouraging. Different types of encryption are readily available, including strong encryption that will not be easily cracked even by very powerful computers. Many people use encrypted internet traffic every day without even being aware of it.

But even if someone monitoring communications cannot see the contents of communication, they can see that it is being used. That may be enough to get journalists and their sources into trouble. For instance, tools that protect the contents of an email may not offer any protection of metadata – information about the nature of the communication including the sender and recipient – and that can be damning enough in itself.

This section will look into the basics of internet traffic encryption and what can be done to protect the content of online traffic from eavesdropping.

3.3.1 Basic encryption - HTTPS

Someone monitoring a network cannot necessarily see everything you do in it, even if you've never taken a single precaution. Many sites use what is known as HTTPS (short for HTTP Secure) encryption. When supported, HTTPS can protect against eavesdropping or tampering with your traffic, but will not anonymise or hide the identity of sites you visit, how long you visit them or home much data you download - only the actual content of the traffic. HTTPS offers some basic protection but it is limited and should not be mistaken for solid security. Using the postcard analogy, HTTPS is an envelope that can, when the site in question allows it, cover your letter but not the address of the recipient or sender.

That said, HTTPS is better than nothing against some threats. For many internet browsers (such as Mozilla Firefox and Google's Chrome) there is also an add-on called "HTTPS Everywhere" that when installed will help activate HTTPS security on some sites. Note though that HTTPS Everywhere works by activating pre-existing HTTPS features in sites; it does not create them or lend protection to sites

that do not have HTTPS functionality. If you want to be anonymous online or advise a source on how to do the same, more protection is needed.

3.3.2 Virtual Private Networks (VPNs)

Another tool to encrypt traffic is known as a Virtual Private Network (VPN). VPNs can, for instance, be used to connect to internal company networks from home or abroad. But they are also used to encrypt internet traffic, altering the user's apparent location, and to obscure the source of traffic to and from a given website.

A VPN creates a tunnel to disrupt the standard travel from A to B. Instead traffic travels from A into the encrypted VPN network tunnel, it then emerges from the "tunnel exit" and proceeds to B, and then takes the same route back. Proxy servers, which are a different and less secure type of intermediaries, have similar functions but usually lack the strong VPN encryption.

VPN's can offer encrypted high-speed traffic, and are available from a great many providers. That said, the provider holds the cryptographic key and could see your traffic. A VPN could, for instance, decide to comply with authorities and pass sensitive data along although many say they do not retain data or hand it over. VPNs may still be a useful option, depending on what potential threats you see to your traffic.

3.3.3 TOR

Anyone that has encountered discussions on online privacy and information security may have heard of the TPR project, or The Onion Router. TOR offers encryption and hides the path internet traffic is taking, offering some but not absolute anonymity. Tor was developed originally in the United States with the US navy in mind, in order to hide and protect US government communications. It still receives most of it's funding from the US. TOR is used by everything from law enforcement and intelligence agents to journalists and political dissidents, as well as criminals.

TOR advocates argue that despite the service being constructed to protect American communications, including that of spies, its open source transparency demonstrates that it does offer a more trustworthy security than non-open source options. TOR works by sending your traffic through an encrypted network where it jumps from one point to another, combining strong encryption with a large degree of anonymity as no single point can see both the origin and destination of the traffic.

It is important to note though that while traffic travelling into and through the TOR network is encrypted, the last step – exiting from network to the final destination – is not encrypted. Anything written in plain text will still be readable, which means that it may be important to also use other encryption to protect the contents of your traffic. It also needs to be mentioned that there have been some concerns about the ability of major powers to eavesdrop on TOR if they control enough nodes in the system from leading TOR developers.

So why not always use TOR? First of all, Tor-browsing can be very slow, as speeds will depend on the capacity of the node servers. Secondly, some countries, especially ones with authoritarian governments, may block TOR access. Thirdly, and importantly, someone monitoring your traffic may be able to see if you are using TOR and as far as conspicuous traffic goes, it is fairly conspicuous. There are examples where merely using TOR has landed individuals in serious trouble.

3.3.4 Emails

Email communication today is ubiquitous. In 2015, the amount of emails sent worldwide in a day topped 196 billion messages. But email messages can easily be both monitored and saved and emails can be vulnerable to hackers. Among journalists, further concerns have been raised as media outlets have adopted cloud-based solutions outside their own physical reach to handle their emails rather than running their own servers.

So what can we do to protect our email? There are commercial options available, but you may also be familiar with the abbreviation PGP (Pretty Good Privacy). It is a well-recognised type of email encryption, commonly used but requiring a bit of practice.

Basically, PGP works by the user generating a random private key that they keep to themselves, and then a public key that can be shared. Messages sent to the recipient are encrypted by the sender using that user's public key, and the recipient then unlocks the scrambled encrypted text using his or her private key.

One simplified way of describing it is that you create a number of locks (public keys) and share them around. Anyone can use one of these to lock a message they are sending to you. But all of these locks can only be opened with one key (private key) that only you hold. When you want to return the email you encrypt it in the reverse direction with the recipient's lock (or public key), and the recipient will unlock the message using their private key.

A common open source PGP version is abbreviated GnuPG or GPG and is compatible with many different types of software programs. Using GPG will offer strong encryption protection for your communications and is one of the most widely used and trusted forms of online communication in circles concerned with serious data security. In many countries, introductory training sessions in PGP use are offered by colleagues or online privacy organisations.

3.3.5 Messaging services

Despite the prevalence of emails, it should come as no surprise that there are today a range of different messenger services available online. Social media sites especially have grown massively and today account for a large share of all internet traffic. From a security perspective however, such sites generally pose serious problems. Aside from the fact that collecting and selling user data is the essence of their business model, it may be difficult to confirm the identity of the person you're speaking with, accounts are easily hacked, and phones easily lost.

There is however an array of messenger services using the "Off The Record" (OTR) protocol that offer a safer option. OTR messengers offer encrypted instant messaging conversations as well as

features to confirm the identity of the person you're communicating with. If you happen to lose control of your encryption keys, previous conversations will not be compromised. Also, after the conversation is over the messages will not carry any digital signatures so you could plausible deny any messages have come from you.

Some examples of OTR chat clients are Pidgin (cross-platform), Adium (OS X), ChatSecure (for mobile devices) and Miranda (Windows). Google's Google Talk service also uses the term "off the record" but does not offer this type of protection.

3.4 On the drive

In the section above we looked at how we can protect our data traffic, but what about what we leave behind on our hard drives and memory sticks? The computer or cell phone of a journalist can contain a treasure trove of sensitive information. The first rule of thumb is to always password-protect any devices you going to use, but this may not help against the determined.

In this section we are going to look at different types of disk encryption that can allow you to protect a computer, file or thumb drive if they would fall into the wrong hands. It is also a good idea to encrypt any data you intend to upload outside your own physical reach, for instance on an online server. And again, encryption will not make your data invisible, only unreadable to anyone without the key. It may still be clear that you are using encryption, in many places itself suspicious enough.

3.4.1 Disk encryption

There are many commercial encryption options available, for instance your computer's operating system, (such as Apple's OSX system) or phone system (such as Google's Android) may well offer the option of encryption. There is also a wide range of alternatives in the market for encryption software that promises to protect your data, bundles of files or hard drive as a whole.

Often commercial software for cryptography will be easily accessible, easily used and offer a strong encryption – depending however on who the perceived threat is. In general, as with standard data traffic, there are concerns about to whom companies can hand over data and the risk of back doors allowing authorities or others direct access to purportedly safe data.

Certainly, the revelations of Edward Snowden have showed many of these concerns to be well-founded. Therefore you need to think about what protection commercial encryption firms actually promise to deliver if authorities ask them to hand over your encryption keys, and if you think they might do so despite promising otherwise.

That said, in most cases there are strong and user-friendly commercial software options available are used for much of what journalists do online. If you require a higher degree of safety, or for some specific reason believe that typical commercial file encryption is not what you need, there are non-commercial licenses.

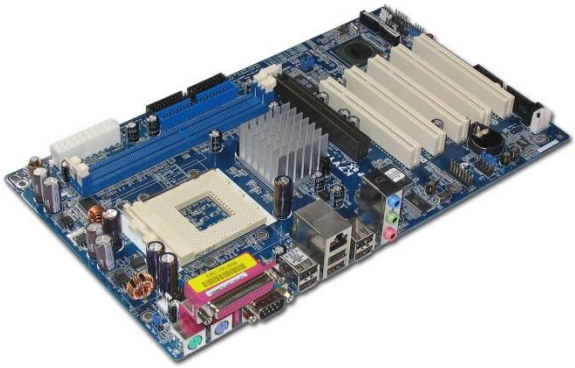
There are several different options but one open-source option that has been popularly used for some time is called TrueCrypt. TrueCrypt has had many advantages including being free to use and

with advanced options for encrypting hard drives, USB-sticks, single files and much more with comparative ease. TrueCrypt was however discontinued during May 2014, and a message posted on its site stated that it may contain unfixed bugs. The discontinuation of TrueCrypt unleashed much speculation both with regards to the reason for this decision, but also with regards to how safe its encryption actually is. However there has been a project to independently audit the software and no specific back doors have been found and made public. Many still use TrueCrypt and unless you believe a major power is coming after your data it is often considered comparatively safe in the sense that it's one of the better options accessible.

Another useful feature with TrueCrypt was that it would allow you to encrypt a file using two different passwords where the content would vary depending on which one you entered. This allows for what is often referred to as plausible deniability. This means that someone who finds the encrypted file and demands you unlock it can be given one password (to a less sensitive or even false content) without jeopardising the "real" content that would only be shown if the other password was entered.

During the end of 2014, alternatives have however emerged, such as CipherShed which is derived from TrueCrypt's code, but where all the code has been made public to comply with open-source guidelines. The individuals behind CipherShed are also not anonymous, which was the case with TrueCrypt. Another similar project, also based on a fork of TrueCrypt is called VeraCrypt, but anyone interested in this will need to inform themselves on what is the latest tool.

3.4.2 Hardware vs Software



A serious concern in any discussion of source protection is how far we can trust any of the devices we use to securely protect our data. This applies both to the hardware, the physical bits and pieces that make up a device, as well as the software, that is the programs we run on that hardware.

Regarding hardware, concerned voices have been raised with regards to what access might be available to the companies that produce them, and by extension authorities that could be granted access. The Edward Snowden revelations suggest that intelligence services have been able to remotely access computers without even needing them to be connected to the internet. Some people physically remove pieces from the computer such as Bluetooth chips, microphones, or cameras out of concern that these could be remotely accessed. While some of these measures may seem extreme, it is useful to at least consider that hardware in computers, phones, tablets, as well routers and other related hardware, may be accessible to exceptionally powerful organisations. As Snowden revealed, this is not a hypothetical situation.

With software, there are different concerns. On one hand, there are concerns that harmful malware programs may be used to spy on computers. Keylogger programs that store the key strokes typed

into a computer, programs that record images from the screen or record conversations in programs such as Skype, or malware that offers direct back door access into the computers operating system – all of these are used by criminals, the casually bored, jealous spouses, and government authorities to spy on individuals. Making sure that the programs you use are updated and that antivirus protection is active are both important, but often users will be fooled into installing these programs themselves through social rather than computer engineering. When that happens no encryption will be able to protect you, and if you suspect your computer may have been infected or compromised you may have no other option than to wipe the hard drive and make a clean install of your operating system.

The second concern with software is wider, and more difficult to tackle. Simply put, it is based on the concern that any software - be it operating systems or other programs - that are not open source and easily audited independently may be vulnerable to eavesdropping. The main concern is that programs may have back door access written into the code that allows direct access, access that may be exploited by the companies themselves, authorities, hackers, or anyone else that gains access. This concern also extends to any encryption that is not open source.

While the closed nature of many commercial programs means that these suspicions often cannot be definitively proven, the Snowden documents reveal that large tech companies have been granting backdoor access and handing over data, arguing that they are legally required to comply. As with hardware, the back door issues are not a hypothetical according to the Snowden documents.

3.4.3 Tails

One option that will not be discussed in detail here but deserves to be mentioned is Tails, a version of the operating system Linux constructed with privacy in mind. Tails is intended to be run from a USB memory stick, a memory card or a DVD disk. It is made to leave no trace on the computer where it is used, and runs all traffic through TOR. It also includes a large number of programs that can be used to encrypt, obscure or otherwise protect data. Tails is an extremely useful tool if high level security is necessary, and anyone interested can access further reading online.

3.4.4 Detekt – Amnesty

For a slightly different perspective, the rights group Amnesty international recently launched the service Detekt to search computers for the most well-known malware risks used by some governments that spy on computers. The background was in part concern that many activists or other people targeted may lack advanced software to fight malware or viruses, or old computers. At the same time it is also about awareness-raising, as the scope of malware that could really be addressed is limited.

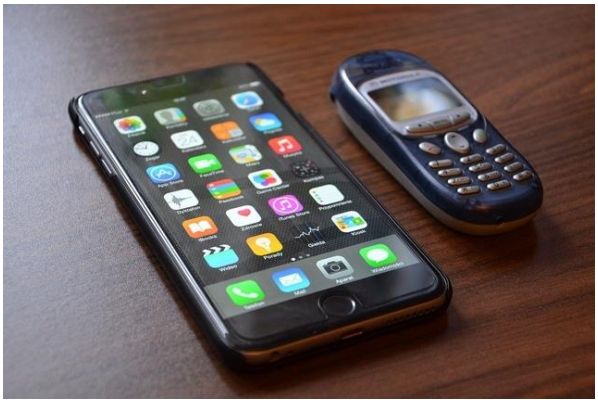
3.5 On your phone

Smart phones with advanced high-definition cameras and high-speed internet services have had a big impact on journalism allowing the telling of stories in new and exciting ways. Unfortunately, there are also risks associated with carrying around small computers that contain not only an array of sensors, lists of contacts and communications, but also make combining this information and

passing it on technologically simple. One absolute must, however, is using a password to protect your telephone. Never have a phone without a passcode of some form.

3.5.1 Phone networks

Much of what you do on your phone generates data by which you can be identified. Call logs from land lines as well as mobile phones are stored. For regular phone calls some kind of court order or permission is often needed if authorities wish to wiretap phone calls. The metadata of your phones calls are often easier to access and can easily be stored over time. French authorities, for instance, have admitted that intelligence agencies obtained detailed lists of calls made by journalists at Le Monde. Not only authorities can do this. In Sweden there have been examples where employers requested the phone call lists of employees using work telephones. In this way calls made from employees to journalists have been revealed, in at least one case leading to an employee losing their job.



From a technical perspective, your mobile telephone, as well as your SIM-card, also carries information that can be used to identify who you are as well as your location. If you need to meet someone in person, agree on a time and place and then leave your phone behind, as someone registering your phone as well as the sources on the same place at the same time is a give-away. Turning the phone off or even removing the battery may not protect you.

In extremely sensitive situations where phone communication cannot be avoided, it is better to meet in person or to buy simple, brand new telephone with unregistered SIM-cards for both your source and yourself. “Burners”, as they are called, are a safer bet, but will still leave traces and should not be kept or used longer than necessary.

3.5.2 Internet traffic

The risks associated with using the internet on your phone are the same as with other internet use, except that phones will usually have access to even more information about you such as GPS location data. Services such as VPNs and Tor, explained in an earlier section, are available for mobile devices however.

A smart phone contains an array of sensors, microphones and GPS. Always make sure to look through the security and privacy options in your phone. Consider turning off, for instance, location services entirely except for when you really need them. This basic level of protection will only however prevent some of the haemorrhaging of data to apps and the companies that make them; it will not prevent someone with remote access to the phone’s operating system or hardware. Similarly, think about whether it is a good idea that apps automatically upload data such as photos online or have access to your saved contacts. Often the answer will be ‘no’.

3.5.3 Encryption

Many phones today do offer encryption of the contents. For Apple's line of iPhones, for instance, your data will be protected on its flash drive as long as you have a password. On Android phones you will often find the option to encrypt under security options. But as with any commercial software, there is no guarantee against access or authorities demanding access from the company. Apple have recently said they will no longer hand over information to law enforcement agencies, but other methods of extraction may make this irrelevant.

3.5.4 Apps

Apps can either help protect your data, or make it vulnerable. As mentioned previously, look through the privacy and security options of the apps you have installed and consider carefully what access they actually need to, for instance, contacts or locations.

Meanwhile, apps such as RedPhone and TextSecure for Android offer encrypted phone calls and text messaging. Similar apps for the iPhone are TigerText and CoverMe. Also worth looking into is SilentCircle's suite, as well as Guardian Project apps that allow internet access via Tor networks, tools for Off The Record messaging, and more.

3.6 Passwords

3.6.1 Strong Passwords

Strong passwords, as well as what is often described as "password hygiene", are essential to any serious attempts at securing your data. It may seem tedious to continuously change passwords, to avoid reusing passwords, and to select passwords that cannot be easily cracked - even seasoned data security wonks can find this challenging – but it is simply a necessity. Different systems can be devised to protect passwords, and while we won't go into detail here, the usual recommendations of choosing many different types of characters are all sensible. And while tools for cracking passwords today are strong, a long password will be much harder to crack than a short one.

It is also useful considering that passwords do not necessarily get hacked using brute technical force, but often by social engineering and tricking people into divulging their passwords. Be extremely suspicious of any requests for your password if you feel the least bit uncertain. Other threats are "keylogger" malware programs monitor your keystrokes, or hackers that manage to get hold of password data from one service and the use your login information to access other services. In short, any hygiene be it password or physical, will take a bit of effort but it is in everyone's best interest that we both wash our hands and choose passwords with care.

3.6.2 Two-step verification

One useful function that more and more online services are allowing users to activate is two-step verification when you log in to your account. It is what many may have been doing for a long time when logging into their bank accounts online, using some sort of digital device that generates a code used to log in. The difference being that most of the time the device you will now use is your phone.

If you do not have two-step verification activated, usually you will enter your login details and your password, and you will be able to access your account. With two-step verification there is, as the name suggest, a second step. Upon logging in to your account, a text message or code will be sent to your selected device (most often your telephone) and you will then need to enter this before your can use your account. Some find that this is somewhat tedious, but it is a small step that will vastly improve security and you can often tell accounts to remember the computer or other device you logged in on so that you will not be asked for a code every time you log in.

Examples of services that employ two-step verification are Google's services (Gmail, Google drive et cetera), Facebook, Twitter, DropBox and Apple's iCloud.

3.6.3 Password managers

Another potentially useful tool is a password manager that will allow you to gather passwords for different services and keep them on one central key-ring. Some of these password manager services will allow you to login directly to the different sites you might be using and also let you copy and paste passwords in order to avoid keylogging malware.

At the same time you are gathering all your keys in one place, as with any key-ring, and if you lose your password or someone else gets hold of it you might be in even worse trouble. As with any programs, at least those that are not open source, there is also the risk of backdoor access available to both the programmers behind the code as well as authorities.

4. What are some current projects?

4.1 Training

While the lack of data security skills among journalists has often been lamented, few schools of journalism offered their students much practical training until recently. One main reason may have been that the skills were simply not there with older generations of colleagues and that there were not the teachers available.

More recently however, as the issue has received greater attention and grown more prominent in the discussion of data security, schools have increasingly been offering at least some basic training in operational data security. Moreover, professional journalists have been able to choose from a growing selection of courses and training opportunities.

One increasingly common tool to boost data security and digital source protection skills for journalists has been targeting professional journalists already in the business. The reasoning has been that active professionals are the ones who these skills the most, and that they are already working and potentially handling sensitive information in an unsafe way. Training sessions are being conducted both hands-on through workshops or programs, as well as online in the form of Massive Open Online Courses (abbreviated "MOOCS") or by other means.

In general, many who train journalists in data security issues describe a growing awareness of the risk at hand, and the need to address these through hands-on training.

Fundamentally however, the skill level in many media organisations is still very weak, according to several of those interviewed with regards to their work in this area. Anders Thoresson, a freelance journalist who has educated professional journalists in Sweden as well as students, describes one case where he asked members of a Swedish local newspaper how many of them had any type of lock screen password on their smartphone. He was genuinely baffled when only half or so said yes:

> *"For God's sake, I asked, don't you have your internal editorial email messages in those? Well yes, they said, but it's so inconvenient to enter it. I thought this was a blanket excuse that no one actually uses."*

Thoresson adds that the realm of data security and digital source protection will be something that older journalists already working will expect from younger journalists fresh out of journalism schools. This opens both for an opportunity for recently educated journalists to offer badly needed skills, but also means that the expectations of recent graduates has increased.

The students Anders Thoresson has been training have mainly been studying at the University of Gothenburg's department of journalism (JMG). JMG is an institution that prides itself on its investigative focus, and has during the recent years increased training in digital security. One striking fact has been that despite belonging to a generation often touted as "digital natives", few if any students in a class understand how the internet works and how to use it more securely, Thoresson says. The main goal is therefore to instil some understanding of internet infrastructure and a security conscious mind-set:

> "*Somehow there's a sense that the internet is a dangerous place but not of how that applies to journalism as a profession. My point when I leave is not that they should have acquired a wide battery of software that will always work, but rather the notion that the internet can be a risky place and that they understand this the day they might need it."*

Arjen Kamphuis, an information security expert who has been working in IT since the mid 1990s, has been training journalists, journalism students in computer security for years. He is one of the authors of 'The Centre for Investigative Journalism Handbook' on information security for journalists and speaks regularly at journalism conferences on issues of information security.

Kamphuis says that he continues to be amazed that most investigative journalists do not appear to have spent any time considering issues of information security, despite all that is now known. He likens the computer skills level of an investigative journalist between 25 and 55 years of age to that of average European 12 year-olds:

"*Apparently not enough people have been arrested or worse in order to wake people up about this…..The more people that do more teaching can only be a good thing, because clearly a lot more training is needed*."

On the other hand, Kamphuis emphasises that the Edward Snowden revelations show that tools such as properly implemented encryption and TOR network usage can allow a high level of security, and that these are things that can be learned. Ultimately, he believes, it comes down to whether journalists are willing to spend a few days learning how to use tools:

"*I've seen journalists do this and I've seen journalism students do this," he says. "It's really all about motivation. The technology certain isn't perfect, but it's now at a level where anyone who wants can learn, can."*

4.2 Handbooks

Another type of material increasingly available for educational or training purposes is the handbook. Examples include *Information Security for Journalists* from the Centre for Investigative Journalism in the United Kingdom, The Swedish handbook *Digitalt Källskydd* produced by the .SE foundation in cooperation with the Swedish Union of Journalists, and *Manual de Seguridad Digital y Móvil* produced by Freedom House and the International Center for Journalists. Other guides, such as the *Journalist Security Guide* from the Committee to Protect Journalists, include chapters on information security and the Electronic Frontier Foundation's *Surveillance Self-Defense* toolkit is kept up-to-date online.

Though varying in size and scope, the basic idea of producing clear and easily shareable guides to digital security is similar and understandably attractive. They are available in several different languages and there is work ongoing to translate several of these into further.

Silkie Carlo, an activist and along with Kamphuis co-author of the Centre for Investigative Journalism handbook, says that the reception has been encouraging and that there is a clear need for handbooks of this type. Some use it pre-emptively, she says, while others will go looking when a situation arises. The former is preferable because acquiring the necessary skills may be difficult in an urgent situation, but it requires careful planning in outreach and presentation. Another issue to consider is what technical skill level to aim for, but Carlo says that accuracy needs to be a priority:

"*We really tried to be thorough, but speak to people who have a reasonable level of computer literacy because otherwise there may not be much of a point. But not compromising with security was the big aim."*

An important additional point, Carlo adds, is that the handbook has been very useful as a complement to face-to-face training, something she has been involved in several times with student journalists as well as working professionals:

"With a trainer and a handbook it gives people the ability to self-teach to the extent they can and only use us for a bit of trouble shooting."

Increasing numbers of universities, trade unions, organisations advocating online privacy, and other groups are offering options in the way of digital security training. There may be face-to-face training available, but also Massive Online Open Courses (MOOCs).

4.3 Dropboxes

One simple solution that may be tempting is the service DropBox which allows you to set up an inbox where files can be uploaded. Dropbox has large advantages in that it is simple, free, and easily accessible on a wide scale. Many people know basically what it is and how to use it.

The disadvantages however, are great. It is unclear exactly how much access Dropbox as a company gives authorities or law enforcement agencies, but the whistleblower Edward Snowden has described DropBox as "hostile to privacy". Dropbox has previously stated that they can and will comply with legal requests to hand over information, which can put journalists and their sources at risk. A source can take their own steps using the TOR network as well as other disk encryption tools to make the transfer of data via a Dropbox substantially safer. But DropBox is not to be considered very protective of those contents if law enforcement comes knocking.

Other examples of encrypted submissions boxed use forms encrypted using HTTPS. One such is "Radioleaks", employed by Swedish public radio. Sweden is particularly interesting because of the high standard of source protection Swedish journalists are required to live up to by law. Radioleaks uses HTTPS technology to encrypt and protect the data traffic of persons uploading information to their site and claim to have received over a thousand tip-offs resulting in over a hundred actual news items, some of them very sensitive. For instance, after Swedish Radio broadcast the award-winning investigation into Swedish arms exports to Saudi Arabia, internal discussion at the Swedish Defence Research Agency about the fallout of the reporting was received via the Radioleaks service.

HTTPS will protect traffic, but it won't disguise who is visiting the Radioleaks site. Beyond that, as with HTTPS licenses in general, there has been much concern since the revelations of Edward Snowden that this system of security may in itself be compromised by exploits or backdoors available to USA and perhaps other powerful intelligence agencies.

Finally, more and more media organisations have been choosing to set up submission inboxes using some form of onion routing based encryption, requiring the user to be connected to the TOR network in order to access the site where the submissions. Different alternatives to TOR have been developed, including "SecureDrop" and "GlobalLeaks".

SecureDrop, originally developed by the late Aaron Schwartz and Kevin Poulsen under the name "DeadDrop", has been receiving quite a bit of attention recently, being used by The Guardian,

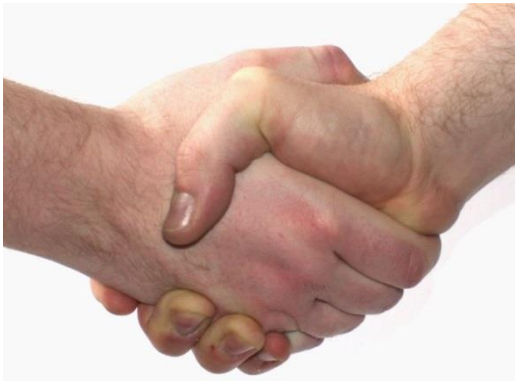
Washington Post, Forbes, and Pro-Publica among others. The New Yorker originally used an earlier version named "StrongBox" but is now using SecureDrop as well.

SecureDrop sites, an official list of which are maintained, are only available to users of TOR. This means that users by definition have to protect themselves and their identity to some degree before they are even able to access the service. The prospective source can then access a separately set up server set up by the journalist or news organisation which does not record information about the visitor's point of origin. The source or whistle-blower also receives randomly generated login information rather than using anything readily identifiable, thereby strengthening the anonymity further.

Data or files received are moved from one computer to another using an USB memory stick. Along with a second memory stick, that contains the encryption key, these are both entered into a computer that is not connected to the internet and there the data is unlocked.

Despite all these steps, media organisations maintain that absolute security is not something that can be guaranteed, only to a greater or lesser extent. It is fair to say that SecureDrop is at least safer than an email, depending of course on what other steps are taken both by journalist and source to guarantee that the data is safeguarded.

4.5 Going old-school



Finally, some journalists interviewed for this report said that they faced with uncertainty about the level of surveillance that they face, or uncertain of how to tackle potential threats, they would prefer not to use digital communication at all. Rather, a return to handwritten notes and verbal communication away from the office seems preferable to a technical solution.

This does not, however, apply only to individuals sceptical to the ability their technical know-how. Arjen Kamphuis, quoted earlier in this report, says there may be extreme cases where this is necessary, if it is based on a sober assessment of the potential threats:

> *"If you're under an extreme level of surveillance,"* he says. *"That may actually be a good assessment of the problem. If you're Julian Assange you won't trust anything with a power plug,"*

But most of us are not under that level of surveillance, he says:

> *"You can defeat almost any adversary on this planet with a little bit of budget and a little bit of time. It can still be done even today, even despite everything."*

5. Conclusions

Given what we today know about the technical surveillance abilities available to powerful actors and the lengths to which they are willing to go regardless of regulation, journalists face a serious dilemma. Are we able to offer sources guarantees of protection as long as we ourselves use digital communication that could potentially be eavesdropped upon?

And given the proliferation of malware and other means of spying and snooping – available not only to governments but also to criminals, employers, the generally curious, and anyone who runs a website – it's not a dilemma journalists can dismiss based on the notion that they are not doing any of that "Wikileaks stuff".

The issue is difficult to resolve for several reasons. One reason is limited technical know-how in the profession as a whole. How can we even start to answer the questions if we do not even have a working understanding of how a computer or the internet actually work?

For some the solution is to avoid digital communication entirely, abandoning online communications and computers and instead reverting to analogue communications. But for how large a share of journalists is this actually an option? For better or for worse, we have grown dependent on digital communication and, importantly, so have our sources.

This being the situation we most likely need to accept that most journalists will be using digital communications, and move forward from there. It is only by equipping journalists with the knowledge and tools to assess how vulnerable their communications are, they can make the judgment calls on a case-by-case basis.

So how best to deliver the education? Is it through targeting students before they enter the profession, to select those in urgent need when they're already working, or offering a blanket solution using freely available research and digital protection handbook?

Stuart Hughes, Senior World Affairs Producer with the BBC points out that journalists in what are considered risky environments are expected to attend training sessions in physical security but not digital security, despite many of us spending more hours connected to the web in front of a screen than in the field. Can that line of reasoning yield an approach that will resolve at least some of these issues?

The purpose of this report is not to answer that question, but rather to introduce journalists to the issues that they may be facing and some initiatives to tackle them. Technological developments will mean that any specific advice or suggestions of tools may soon become irrelevant and so it is up to each journalist to stay abreast of developments that affect their privacy. We hope that this report takes one step towards increasing awareness around source protection in a post-Snowden age and provides a starting point for journalists to educate themselves, seek out training and protect both their data and their sources.

Acknowledgments

This report was written by Swedish journalist Carl Fridh Kleberg.

The author would like to extend his gratitude to all the people who made this report possible, including all those interviewed of whom many we were unfortunately not able to quote in this text. Special thanks go to the Swedish Journalistfonden foundation and the brilliant, professional, and patient staff at Polis, LSE especially Director Professor Charlie Beckett. The opportunity has been a true privilege.

We are grateful to the support from the Swedish Journalistfonden which supported the research carried out at Polis, the journalism think-tank at the London School of Economics.

May 2015