Deep Web for Journalists:
Comms, Counter-surveillance, Search

Special Complimentary Edition for Delegates attending the
28th World Congress of the
International Federation of Journalists

*

By Alan Pearce
Edited by Sarah Horner

*

www.deepwebguides.com

Table of Contents

Introduction by the International Federation of Journalists
A Dangerous Digital World
What is the Deep Web and why is it useful to Journalists?
How Intelligence Gathering Works
How this affects Journalists

1 SECURITY ALERT
- Setting up Defenses

2 Accessing Hidden Networks
- Using Tor
- Entry Points

3 Secure Communications
- Email
- Scramble Calls
- Secret Messaging
- Private Messaging
- Deep Chat
- Deep Social Networks

4 Concealed Carry

5 Hiding Things
- Transferring Secret Data
- Hosting, Storing and Sharing
- Encryption
- Steganography – hiding things inside things

6 Smartphones
- Counter-Intrusion
- 007 Apps

7 IP Cameras

8 Keeping out the Spies
- Recommended Free Programs
- Cleaning Up
- Erasing History
- Alternative Software

Share the Knowledge

About the Authors

Foreword by the International Federation of Journalists

Navigating the Dangerous Cyber Jungle

Online media safety is of the highest importance to the International Federation of Journalists. After all, the victims are often our members.

The IFJ is the world's largest organization of journalists and our focus is on ways and means to stop physical attacks, harassment and the killing of journalists and media staff. In an age where journalism – like everything else in modern life – is dominated by the Internet, online safety is emerging as a new front.

In this new war, repressive regimes now keep a prying eye on what journalists say, write and film. They want to monitor contacts and they want to suppress information. For journalists, this has become a dangerous game of cat and mouse.

Journalists are on notice – "everything you say and write will be taken down and used to track you and your contacts down."

This merciless pursuit for control of online communications has considerably raised the stakes in the current safety crisis facing journalists and the media. We are living at a time of unprecedented levels of violence against the Press.

Now we need to master the skills necessary to navigate this dangerous cyber jungle.

'Deep for Web Journalists' is the tool to achieve that. This engaging book by Alan Pearce charts a path to online knowledge which should be compelling reading for all journalists.

It offers an uncompromising diagnosis of the perils of online communications and should shatter the confidence many of us place in the unguarded ways of working online. This book offers simple advice to cover our tracks online and ensure that journalists are not an easy target for online press freedom predators.

Read all about 'Deep for Web Journalists'!

Jim Boumelha,

President, International Federation of Journalists

This is an abridged version of 'Deep Web for Journalists: Comms, Counter-Surveillance, Search' by Alan Pearce

A Dangerous Digital World

Being a journalist in 2013 is more dangerous than it ever was. In addition to the usual threats, beatings, murders and war casualties we are now being actively targeted online by intelligence agencies and law enforcement.

These days it is not just journalists working in repressive regimes that need worry. Increasingly, outwardly-democratic governments are tightening control over the Internet and those who use it.

All sophisticated security services monitor Internet traffic within their own countries. The US monitors all Internet traffic if it passes through US-owned "processing services", which the bulk of it does.

Legally, just the bare bones of the communications are monitored – the who sent what and when. But, although they may not be open about this, many agencies are now looking directly into the message itself, looking for the expected and the unexpected in all our online communications and activities.

But don't suppose actual agents are used for such mundane tasks. Algorithms of stunning complexity analyze literally every word. And, when certain triggers are pulled, the surveillance moves up a notch and so on until it enters the physical world.

Journalists are prime targets. They have contact with politicians and activists, they have their finger on the pulse and they are capable of causing all kinds of trouble both to governments and to corporations.

If they become interested in you, they will monitor all your online activities and read your email. They will see who your contacts are and they will start to monitor them, too.

Knowing how to protect yourself online is just as important as knowing your law or how to operate in a hostile environment. Yet, surprisingly, many journalists leave themselves wide open.

Cybercriminals use the same techniques, drawing people to a webpage where malware will automatically plant itself in the computer, known as a "drive-by download".

But, as daunting as this may seem, most threats can be overcome without any real technical skill. Using freely downloadable programs and apps, you can block intruders, mask your identity online, set up secure communications, and transfer and store any amount of data without anyone being any the wiser.

…and getter ever more dangerous

Today everything is connected, everything communicates and everything is a sensor. Technology is moving so fast that even the major intelligence agencies can't keep up. Put all these things together and the inanimate becomes sentient and capable of decision-making. Suddenly the great dystopian fear is a reality.

Later this year, the Community Comprehensive National Cybersecurity Initiative Data Center in Utah will be on-stream, capturing all communication globally, including the complete contents of private

emails, cell phone calls and Internet searches, plus all the personal data trails from parking receipts, bank transfers, travel itineraries and bookstore purchases.

And this is how they will profile us all. It's been happening for years in the commercial world. Only now, when you appear to step out of line, say the wrong thing or spend too long looking at a bad kind of wiki, will you become interesting to the suspicious minds.

But, as it turns out, the bad guys don't say *kill* or *bomb* in their emails or on Twitter. The terrorists and super-criminals can also hire the smartest brains in the IT world and they pay better.

According to the US National Academy of Sciences, whilst data mining may work in the commercial world, it simply isn't feasible to prevent atrocities because terrorists don't use a one size fits all model; they change and adapt their *modus operandi* as they go along, preventing the algorithms from picking out a pattern.

Curiously, governments and intelligence agencies know this, too.

What is the Deep Web and why is it useful to Journalists?

Simply put, the Deep Web encompasses everything that the conventional search engines can't find. Google may index around 15 billion pages but it only seeks out those that want to be found or have conventional addresses that end in *.com* or *.org*, etc. It skims the surface and offers up the most popular results.

Largely unnoticed by most users, the Internet has been quietly evolving into a vast un-indexed data store. As a result, this Deep Web is so mind-bogglingly huge – some say more than 5,000 times the size of the Surface Internet – that it is both easy to get lost and to stay hidden.

Within this Deep Web are an unknown number of hidden networks; one of which is Tor, a dark world of anonymity. Here, people may communicate secretly and securely away from the attention of governments and corporations, scrutinize top secret papers before WikiLeaks gets them, and discuss all manner of unconventional topics.

Ironically, Tor – which stands for The Onion Router – was set up with funds from the US Navy at the start of the Millennium as a means of covert communication. So dark and murky is it, that other agencies now use it, as do most serious criminals.

Tor has its own websites, chat rooms, forums, blogs, file hosts, social networks and other features of the Surface Web. It is very easy to run into arms dealers, drug cartels, spies, pedophiles, kidnappers, slave traders and terrorists. You can buy top grade marijuana direct from the grower, trade stolen credit cards, buy the names and addresses of rape victims, or arrange the murder of an inquisitive reporter or pernickety judge – and then pay for it all with the Deep Web's own currency, the untraceable BitCoin.

Generally, this is why the Deep Web has a bad reputation. But it has positive aspects, too. There are many journalists who use Deep Web tools like the German Privacy Foundation's PrivacyBox to communicate securely with whistle blowers and dissidents. Aid agencies use similar techniques to keep their staff safe inside of authoritarian regimes.

The Deep Web is also a largely-unknown research and information resource, a goldmine of knowledge lodged in the databases of academic institutions, small businesses and corporations, research establishments, galleries and governments. If you know the right entry points, you can mine a rich seam of multimedia files, images, software and documents that you cannot find on the Surface Web (see the full edition of Deep Web for Journalists: Comms, Counter-Surveillance, Search).

How Intelligence Gathering Works

While some people believe the Internet has set them free, others fear we are all voluntarily plugged into the finest surveillance apparatus ever devised. But let's be clear about this: everything we do in the digital world is open to scrutiny by suspicious minds because that's the way intelligence agencies work. If they didn't make use of this amazing opportunity, they wouldn't be very good at their job.

According to the US Government Accountability Office, back in 2004 there were 199 separate data mining programs being run by 16 Federal agencies on the look-out for suspicious activity.

By 2010, *The Washington Post* concluded after a two-year investigation that there were around 1,200 government agencies and 1,900 private companies working on counter-terrorism, homeland security and other domestic intelligence programs from within thousands of secret data processing sites and "fusion centers" that constitute an "alternative geography of the United States".

The National Security Agency (NSA) intercepts and stores the data from nearly 2 billion emails and other communications each day in its attempts to predict crime in what it terms the "paradigm of prevention" or "predictive policing"; and each day more than 1,600 people have their names added to the FBI's terrorism watchlist.

The US National Counterterrorism Center collects information on *every* US citizen and mines it for terrorism indicators. It then passes on much of this data to other government agencies and increasingly to corporations like Lockheed Martin, Raytheon, CenturyLink and AT&T.

Agencies like the CIA collect all the data they can and then they store it indefinitely. If they ever need to join the dots, it helps to have all the dots from the past to draw upon.

Tracking people in cyberspace is child's play, especially when more than half of all Internet users have a page on Facebook. Big Data – Social, Mobile and Cloud – has altered the flow of information, overtaking traditional media. With commercially-available software like Raytheon's social media data mining tool RIOT, simply enter a person's name and up pops a colorful graph showing where they have been, who they met and what they all look like. It then predicts their future movements.

Trackers are everywhere. Pay a visit to Twitter or Facebook and they will instantly plant little robots that follow you around, noting everything you do. The FBI were recently caught planting trackers in a survivalist website to keep tabs on visitors.

To scoop up everybody else, the agencies channel users through a series of 'black boxes' or inspection points scattered around the net which then read everything that passes through them, analyzing it, logging it, storing it for deeper examination, or marking it for further attention.

With this so-called Deep Packet Inspection (DPI), all Internet traffic can be read, copied or modified, as can websites. DPI can also see who is uploading or downloading, what is inside and who is looking for it. Websites can be blocked and so can specific items within sites such as a particular video on YouTube.

Russia recently authorized DPI, ostensibly to trap pedophiles and prevent terrorist attacks, but some fear with the added ability to delve deep into its citizens' emails and watch everything they do online.

When Iceland recently announced a ban on all Internet pornography, it set its hopes on DPI. But many also fear that the laudable aim of safeguarding children might just as easily be turned to suppressing internal dissent or to tracking down tax-dodgers in straightened financial times.

Generally, ISPs and most governments can examine the 'header' of a message, seeing where it came from and where it's going, but they have not been able legally to peer inside. DPI has been used for years in the commercial world but only Tunisia, China, Iran and Kazakhstan legally use the system to curb dissidents.

Data storage is remarkably cheap and getting cheaper every year. Analyzing and storing it all is now a cost-effective reality. The CIA, which endeavors to collect all data and store it indefinitely, admits that "it is nearly within our grasp to compute on all human generated information."

How this affects Journalists

A reporter working on a story about a local man with an idea to counter IEDs (improvised explosive devices) would very likely read up on military statistics, watch a few explosions on YouTube, check out the different detonators and view an extremist website or two. He would be asking for trouble.

From that day on, the reporter would be a marked man or woman. They could no longer research in private or correspond in confidence. They would never be able to protect the anonymity of a source.

What they could have done, however, was install a few free, tried and tested programs and tweak their computer and smartphone. They could easily have masked their identity and location. And they could ask questions without Google or the NSA building a profile on them.

Rather like spies in a James Bond movie, journalists have an array of digital tools to call upon, both to mask their identity and to provide real confidence that their correspondence, notes and contacts are secure.

There are smartphone apps that let you see in the dark or measure the height of a building. You can film and record without being rumbled; scramble your calls, send emails and other messages that cannot be intercepted or read.

With any modern device you can access banned websites and take over and control public and private security cameras. You can continue tweeting when the authorities take down Twitter locally. You can pass on and store documents away from prying eyes. You might even hide news footage of a massacre inside a Beatles track on your iPod while you slip across the border.

1. Security Alert

Your computer knows everything about you. It knows where you go, who you meet, what you read and watch, and it makes a note of everything you say. It then passes on this information to marketing companies which then sell your detailed profile on to advertisers and political campaigners who in turn micro-target you wherever you go. Increasingly, governments want the same information.

If you are conducting sensitive research or just your normal day-to-day activities, it is advisable to make a few, simple adjustments.

Setting up Defenses

Browser — arguably the most security-conscious browser is Mozilla Firefox which has a large number of free add-ons to help you beef up security. You can switch between regular and private browsing by clicking the Firefox logo in the top, left-hand corner. This will prevent your computer from logging your activities but it will not make you invisible.

Spend a minute or two tweaking with the *Settings*.

- Click the Firefox logo and select *Options*, then *Privacy*.
- Tick the option *Tell websites I do not want to be tracked*. There is an option to *Always use Private Browsing mode.* Untick *Accept cookies from sites*.
- Under *Content*, untick *Enable JavaScript*. You can always switch it back on when necessary because some sites will insist on it.
- Under *Add-ons*, *Plugins* disable the Java Deployment Toolkit, Java Platform and/or Java Applet Plug-in.
- Under *History*, select *Never remember history*.
- On the *Advanced* tab, tick *Never check for updates*. Tick *Override automatic cache management* or set Cache Size to 0. Under *Update*, disable *auto updating/checking for updates*. Update manually from time to time and keep an eye on what it would like to install.
- Under *Security*, tick *Warn before installing add-ons*. Remove all exceptions.

Block Baddies — use either the free or paid-for versions of AVG or Avast which both warn of and block viruses and spyware entering your machine from malicious websites and emails (see Keeping out the Spies).

Force HTTPS — Hypertext Transfer Protocol Secure (HTTPS) is used for secure end-to-end communication. HTTPS Finder for Firefox automatically detects and enforces HTTPS connections when available, providing a reasonable guarantee that you are communicating with the intended website and not an imposter, plus ensuring that communications between the user and site cannot be read or forged by a third party.

Kill Trackers — Do Not Track Me blocks web beacons and trackers that monitor browsing habits. Once installed, a tiny icon in the top right corner of Firefox issues an alert whenever a site has a bead on you. Twitter and Facebook, for example, will try to insert trackers that follow you all over the

Internet, allowing them to build a detail profile of your movements and interests. If people ever wonder how the social networks make money, this is how. To see just who has a commercial interest in what you do online, DNT+ publish a comprehensive list of the companies involved, together with information on them.

Control Cookies — BetterPrivacy allows you to remove or manage cookies and gives various ways to handle Flash-cookies set by Google, YouTube, eBay and others. Privacy+ does much the same thing. Flash plugins run independently of your browser and bypass any proxy configurations. If you were trying to mask your identity, these will reveal your IP address which in turn will point to your physical address.

Java Switch — QuickJava allows you to quickly enable and disable Java, JavaScript and other intrusive plugins which track your travels and preferences. Another good option is NoScript.

Cache Control — the Empty Cache Button adds a button to Firefox allowing you to quickly empty your browser cache should anyone start looking over your shoulder and optionally reload your page with just one click.

Password Protect — KeeFox is a simple and secure password management plugin for Firefox.

Avoid Detours — to stop websites opening other pages on your browser and taking you off to potentially harmful sites, try Redirect Remover which prevents redirects from links and images. Another good option is RequestPolicy.

Control Ads — Adblock Plus allows you to block on-line ads from anyone you would rather not hear from. You can choose from a predefined list and you can personalize your own, but don't block sites you use regularly. Amazon, for example, is so stuffed with ads that by switching them off, the site instantly turns to text-only. You can also customize the settings to remove the annoying ads at the beginning of streaming videos on YouTube and elsewhere.

Secure Download — DownThemAll uses the FireFox safety settings and so requires no configuration and features an advanced accelerator that speeds things up considerably. You can pause and resume downloads. It also allows you to download all the links or images on a webpage and customize the search criteria. It offers the ability to download a file from different servers at the same time for additional security. Privoxy is a web proxy service that fetches items (webpages, images, movies, etc) and passes them on to you when complete.

Search Engines — obviously, Google keeps detailed records of your search queries so select an engine which won't store your records. Options include the Secret Search Labs engine and iXQuick.

Wear a Mask — you can't beat cloaking your identity as one of the safest of all strategies. This way no one need know who or where you are. The simplest solution for quick, anonymous browsing is to use a facility such as AllNetTools and Guardster. These free services allow you to type in any web address and then travel around without leaving a trace of your activities or giving away your location. These are particularly useful for sensitive search engines queries and for visiting locally banned websites.

You can set up a proxy – which gives the impression that you are in another place – by fiddling with the *Settings* in Firefox and changing the IP address to one provided by HideMyAss or Rosinstruments but this can slow your machine down. A simpler solution is Stealthy, a Firefox add-on which seeks out the fastest proxies available and automatically routes you through them.

A very good and more secure alternative is a Virtual Private Network (VPN), effectively a 'secret tunnel' where all your on-line activities are screened from the service provider and eavesdroppers. Free versions include FreeVPN and ProXPN. A popular and fast paid-for option is VrprVPN.

Regularly backup all data, either to a separate storage device or to a Cloud service you can trust, such as those run by Trend Micro and Avast.

If it's not too late, never post any personal information – birth dates, family connections, location, travel plans, identifying photographs, etc – on the social networks.

All this is good for safe activity on the Surface Web but it is not 100% secure. To tighten security further you need to access a hidden network and then add-on a range of simple security options.

2. Accessing Hidden Networks

Tell someone that you know how to go off-radar on the Internet and as a rule they won't believe you. They imagine the intelligence agencies have state-of-the-art technology and can see everything you do. This is only partially true. They do have amazing technology but they can only see things if they know where to look. Down in the Deep Web, by mixing and matching different technologies, you can stay out of sight and make it seriously difficult for any adversary to locate you.

There are several hidden networks. They may be hundreds but nobody knows for sure. We are going to access the most user-friendly – Tor.

First you need a specially-configured web browser to divert your traffic through a worldwide volunteer network of servers. This conceals your location and your activities, effectively hiding you among all the other users. Tor works by encrypting and re-encrypting data multiple times as it passes through successive relays. This way the data cannot be unscrambled in transit.

Tor does have its flaws and should not be considered completely safe. Although your IP address is concealed, a digital fingerprint can linger allowing someone accessing your local network – a Wi-Fi provider or an ISP working with criminals or law enforcement – to glean some idea of your activities.

However, the waters can be muddied for any eavesdropper by requesting more than one site at a time or by downloading more than one item simultaneously, and by regularly re-setting the *Use a new identity* facility on the Tor control panel.

Certain plug-ins will not work on the Tor browser such as Flash, RealPlayer and QuickTime as they can be manipulated into revealing an IP address.

Begin by downloading the free Tor/Firefox bundle. This is safe and easy to install. Simply follow the on-screen instructions and a gateway to the Deep Web can be configured in minutes with no special skills.

Be absolutely certain that you are downloading from the torproject.org website. A hidden network used in Iran was recently infiltrated when a fake version of their modified browser was distributed which gave away the identity of users.

As soon as Tor opens the Firefox browser, be absolutely certain to adjust the security settings as described above. Once loaded, the browser will display a very basic-looking webpage and the words:

Congratulations. Your browser is configured to use Tor.

Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously.

Where is says '*Your IP address appears to be…'* are a set of numbers that in no way connect to your computer. You are now anonymous and free to explore Tor or branch off to the Surface Web.

If you are in a country where ISPs or the government block the Tor network, open *Settings* on the Tor control panel, select *Network*, and then tick the box *My ISP blocks connections to the Tor network*. You are now given the option to *Add a Bridge* or *Find Bridge Now*. If no bridges (non-public

relays) are found, go to the Tor bridge relay page on the Surface Web and select them manually by cutting and pasting until you find one that works for you. Add as many bridges as possible as this increases your chances of connecting and improves security.

Using Tor

On Tor, people communicate secretly and securely. Whistle blowers and dissidents, activists and journalists, aid-workers and academics, criminals and terrorists, and rather a lot of librarians, all carry on their day-to-day activities.

Top secret papers are posted here, as are guides and wikis for every type of activity, legal and otherwise; and all manner of unconventional views are expressed. Here you can lurk hidden and surreptitiously store any amount of data for free.

This is pioneer territory with very few settlers; perhaps 400,000 daily users at best compared to the 2 billion plus who stay up top. Some of the natives are hostile because they would rather keep the place to themselves. Others are friendly because they know more users mean more people to hide amongst.

Deep Websites can disappear or fail to load from time to time. If you have difficulty opening a particular page, just try again later and it may reappear. Links in this ebook marked <!> can only be opened with a Tor-enabled browser. Deep Website availability can be checked at *Is it up?* <!> http://zw3crggtadila2sg.onion/downornot/

Entry Points

- The Hidden Wiki <!> http://kpvz7ki2v5agwt35.onion/wiki/index.php/Main_Page — often described as the hub of the Deep Web, this is the best starting point for new-comers. Here you can find lists of other hidden networks and links to black market goods and financial services, file hosts, blogs, forums, political groups and whistle-blowing boards. The wiki is available in 17 languages.
- Tor*Dir* <!> dppmfxaacucguzpc.onion — simple gateway into the Tor network broken down into categories, such as *Activism, Libraries, File Sharing, Blogs, Security, Adult, Gambling*, etc. At the top of the page is a search facility.
- Tor*Link*s <!> torlinkbgs6aabns.onion — links directory where you can add your own links and set up a Deep Website.
- Silk Road <!> http://silkroadvb5piz3r.onion/ — anonymous black market.

3. Secure Communications

Email — unencrypted email can easily be read or altered by someone with access to any of the computers along the route followed by the email. However, be warned that if you are being monitored the fact that you are encrypting your email or attachments will ring alarm bells and open you to deeper inspection.

Equally, if someone can access your computer, they may change your encryption codes, either denying you access or leaving you with the impression that your data is safe. They may also impersonate you and send out bogus messages. And, while 99% of mathematicians will agree that modern encryption tools cannot be cracked, there are others in the intelligence community who believe they can.

That said, PGP (Pretty Good Privacy) Public Key Cryptography is the standard program for secure email and file encryption on the Internet.

There are two free programs that you can run directly from your computer either as a standalone program or as an add-on to your dedicated emailer – GnuPG and PGPi – but these can be a little tricky to set up. Equally, those with Windows 64-bit machines may find that many programs freeze or crash. A stable, commercial PGP version is available from Semantec that apparently works on Windows 7.

However, there is a very simple online version at iGolder.com. Here you can generate both private and public keys, encrypt a message with your new PGP key, and decrypt messages sent to you.

There are easier alternatives, including signing up anonymously (preferably using Tor or a VPN to mask your location) with a web-based free email service and using that account for sensitive correspondence. Additionally, you might consider only accessing this email from a device other than your own, such as a cybercafé or public library (see Concealed Carry). Always remember to log-out at the end of the session.

If you need to send an email that positively cannot be traced back to you, there are numerous email re-mailing services such as AnonyMouse. Re-mailers strip off any codes that identify you and add new ones along a multiple journey. When the email arrives at its destination, it cannot be traced back to you. This, of course, means they cannot reply. However, you can then give them an alternative means of contact.

A very simple option is to open a free email account and then give the address and log-in details to the other party. Messages are then written but saved as *Drafts* and never sent. The draft messages are then accessed by those with the password. This way the emails are never actually transmitted so are not easily intercepted. Be sure to change addresses regularly as over-active *Draft* boxes can arouse suspicion.

JumbleMe is a paid-for email service that offers several smart security features. Accessed via the system's website or with an Outlook plugin, JumbleMe automatically encrypts emails between subscribers and prevents unauthorized access. Printing, copying and forwarding can be disabled, message recovery can be prevented after a set period and you can limit the number of times an

email can be read. Best of all, emails that have already been sent can be rendered unreadable at the push of a button.

Scramble Calls — one of the best options for secure peer-to-peer telephone and video calling is Silent Phone which allows you to make secure encrypted phone calls all over the world, over any network – 2G, 3G, 4G and Wi-Fi. Silent Phone connects directly to a custom-built secure network for HD sound and vision and utilizes ZRTP Protocol software by Phil Zimmermann, the inventor of PGP encryption. Each user receives a private encrypted 10-digit phone number. Easily integrates existing contacts on your device and works on smartphones and tablets (iPhone, iPad, Android, Galaxy and Nexus).

Secret Messaging — PrivNote is a free Surface Web-based service that allows you to send top secret notes over the Internet. Write a note and it will generate a link. Copy and paste the link into an email or PM and send. The recipient then clicks the link to see the note in their browser. The note then automatically self-destructs which means no one can read the note again, and the link dies. You can choose to be notified when your note is read.

Private Messaging — often shortened to PM or instant messaging (IM), is similar to an email but is used to communicate on Internet forums, bulletin boards, social networks and chat rooms. Tor has several PM options, including PrivacyBox <!> http://c4wcxidkfhvmzhw6.onion/index.en.html which is aimed primarily at journalists. Send and receive anonymous encrypted messages via Tor and on mobile devices. Free service from the German Privacy Foundation.

Deep Chat — online chat covers any kind of communication over the Internet that offers a real-time direct transmission of text-based messages from sender to receiver. Online chat includes point-to-point communications and multicast communications from one sender to many.

- Tor*Chat* <!> http://lotjbov3gzzf23hc.onion/index.php/group/torchat — peer to peer instant messenger providing very strong anonymity. Easy to use without the need to install or configure anything.
- EFG Chat <!> http://xqz3u5drneuzhaeo.onion/users/efgchat/index.php?chat=lobby — secure, simple and easy to use.

Deep Social Networks — the Deep variety of social networks offers the same ability to share photos, videos, audio, etc, but securely. Deep Web social groups include:

- Tor*StatusNet* <!> http://lotjbov3gzzf23hc.onion/ — Twitter clone on Tor.
- Tor*Book* <!> http://ay5kwknh6znfmcbb.onion/torbook/ — like Facebook but Deep.
- Tor*Square* <!> http://ay5kwknh6znfmcbb.onion/torsquare/ — anonymous board, share posts and discussions.

- Tor*Project* Users Group <!> http://lotjbov3gzzf23hc.onion/index.php/group/tor — micro-blogging service that allows users to share short messages.

This will provide a very good level of security but there will still be traces of your activity on the computer. To get around that, we need to take a few tips from James Bond.

4. Concealed Carry

To be extra safe, access Tor directly from a USB drive, SD card, portable hard drive or CD/DVD. These can be used on any Internet-ready computer. Install Tor/Firefox and other useful programs directly to the drive or card and then encrypt it.

A dialogue box to the drive will open as soon as the device is slipped into a computer. Select *Start Tor Browser* and you will leave no helpful trace of your web journey on the machine and no one should be able to track you. If you need to bypass administration restrictions, install FreeOTFE Explorer on the drive and you should be able to get into most machines.

There are numerous tools including the open-source FreeOTFE which uses on-the-fly encryption, meaning data is automatically encrypted and decrypted without you having to do anything except enter a password. When installed, your USB drive will contain an encrypted volume where you can store sensitive data.

In the United Kingdom and Australia, recent laws oblige journalists under investigation to hand over their passwords or face a prison term comparable to that of carrying an illegal firearm. What you need here is "plausible deniability".

There are ways of encrypting files so they do not look like encrypted files; rather they look like files stuffed with seemingly random data. A good option is TrueCrypt, a free open-source encryption program that runs on most operating systems.

You can store your own passwords in a variety of ways. There are dedicated password safes that allow you to manage all your passwords in one place so you don't have to keep remembering different ones or, worst of all, use the same password for everything.

If a password safe can itself draw attention, you can hide passwords very simply by putting them in files where nobody is ever likely to look. Open any program and insert a file deep inside with an innocuous name, such as *Packets29T.txt*.

To produce passwords that cannot be cracked, use an online password generator.

Be sure to update software regularly to maintain security levels.

Free Portable Apps

- PortableApps.com — wide range of open source software for portable devices.
- KeePass Portable — portable version of the KeePass Password Safe. Securely carry your email, Internet and other passwords.
- Notepad Portable Text Editor — Notepad text editor with support for multiple languages.
- VLC Media Player Portable — portable version of the popular VLC player.
- IrfanView Portable — graphic viewer for Windows.
- GIMP Portable — Windows image editor.
- Sumatra PDF Portable — lightweight PDF viewer.
- Eraser Portable — securely delete files and data.

- 7-Zip Portable — portable version of 7-Zip. Works with compressed 7z, ZIP, GZIP, BZIP2, TAR, and RAR files.

5. Hiding Things

Transferring Secret Data

Whenever journalists are arrested, the authorities are quick to remove computers, smartphones and storage devices for examination by forensic investigators. Rather than store sensitive data or contacts on your computer, upload to an online file store either on the Surface Web or within Tor and then wipe all traces with a program like the Heidi Eraser.

It is also important to remove sensitive data from laptops and smartphones, etc, when on assignment and store it on a detachable drive or SD card.

Individual files, such as text or images, can be placed inside a RAR or 7z file and encrypted. Large files, such as *AVI, DivX*, etc, should be split into several components before uploading. Use HJSplit, a free program that both splits and re-joins large files.

For additional security, do not upload all the component parts to the same server/host as they may be spotted and opened. Instead, upload to as many different servers/hosts as possible. Give each part a different name. Remember to rename them in the correct order so they can then be un-split. Do not give the files any name that identifies the content.

Hosting, Storing and Sharing

- PasteOnion <!> http://xqz3u5drneuzhaeo.onion/users/boi/ — paste and share text, images, etc. You can make your paste public or set a password. This is also a good spot to pick up leaked documents. Equally, you can set up a simple Deep Web page here by constructing the page in Photoshop and saving as a *.jpg* which you then upload.
- Onion File Sharing - <!> http://f3ew3p7s6lbftqm5.onion/ — basic file sharing.
- sTORage - <!> http://utovvyhaflle76gh.onion/ — basic file storage.
- QicPic <!> http://xqz3u5drneuzhaeo.onion/users/qicpic/ — simple and swift. Upload any type of file. Caches and compresses uploaded files to decrease loading time.
- OneSwarm — P2P file sharer where you can select who to share with.
- Pastebin — share text on the Surface Web for a set period of time.

Encryption

The safest route for encryption is to encrypt the entire system drive, rather than individual files. Computer forensics can reveal a lot about your computer usage from the system partition including browsing history, bookmarks, emails and contacts details.

Investigators tend to focus heavily on contacts so it is important not only to protect yourself but those you are in contact with. If the investigator cannot access the hard drive their job is so much more difficult.

TrueCrypt — free open-source disk encryption software for most operating systems. Encrypt files or entire drives, including USB drives, etc. An advantage of open-source TrueCrypt is "plausible deniability", meaning no one can prove if a partition or device is encrypted because the files, folders or drives appear to be filled with random data. However, TrueCrypt is vulnerable to some forms of attack. Be certain to read the security warnings first.

Steganos Privacy Suite — not free but a very popular, easy-to-use option that locks and encrypts drives or documents and photos, secures USB drives, CDs and DVDs, organizes and manages all passwords and access information, and shreds data so it cannot be reconstructed by recovery applications. Also includes Internet trace destructor.

Free Encryption Software:

- Kruptos 2
- Folder Lock
- Safe House
- Cypherix

Also see Email Encryption.

Steganography – hiding things inside things

Imagine receiving an email with a harmless photograph of your cousin on vacation with her fiancé. But, known only to the two of you, there is a secret message hidden inside the image. This is steganography, the dark cousin of cryptography.

Steganography is the art of writing hidden messages in such a way that no one suspects the existence of the message. It comes from the Greek word *steganos* meaning *concealed writing* and its use goes back to the dawn of time. Think of invisible ink.

These days you can hide almost any kind of digital file by embedding it inside another digital file, such as *a .jpg, bmp* or audio file.

Sensitive footage that needs to be physically smuggled out of a country can be hidden inside a music track on an iPod or smartphone. Secret documents can be embedded inside a photo.

Counter-technology isn't very good and there is little to give the game away unless the file is unexpectedly large. Just looking at the image or trying to open it with a steganalysis program will not show that the image contains any hidden data.

There are many data hiding packages and services available for every operating system. OpenPuff is a good free program. A good source of information is the Neil Johnson website.

Simple messages can be hidden inside photos posted on Facebook with Secretbook, a free app for the Google Chrome browser.

6. Smartphones

If you want to be monitored 24/7 and followed wherever you go, buy a smartphone.

Threats come in three main forms – SMS Trojans, adware, and exploits to gain control of the device. Smartphones can also be infected when connected to compromised computers and vice versa.

Additionally, law enforcement may oblige the service provider to remotely reprogram a phone's air card allowing for precision tracking. This technique, generically known as 'stingray' or IMSI catcher, allows agents to spoof a legitimate cell tower and trick the smartphone into connecting directly to the stingray.

The majority of malware comes hidden inside seemingly harmless apps which run in the background and collect data all day long. Malicious programs have been detected in apps on Google Play and the App Store for iOS.

They will track your locations, browsing and downloads, and collaborate with other running apps to build up a detailed profile. Some will intercept incoming calls or activate the microphone. Many apps harvest contacts, some collect passwords, while others send secret messages to premium-rate numbers, running up your charges. Worse still, there are apps that run even when the phone is switched off.

Most apps are free or very cheap because developers make their money by allowing in ad networks and other malevolent parties. Be alert when an app asks permission to use your current location – many don't bother to ask – and never give out email addresses.

A growth area in mobile malware is SMS spam where unsolicited messages plant Trojans that hijack the device or just trick users into revealing personal information. As with email and social networks, never open attachments or follow links unless you know them to be safe.

Counter-Intrusion

For Android users, a good free option is AVG Mobilation which protects against viruses, malware and spyware. It also identifies unsecure device settings and advises on how to fix them; ensures contacts, bookmarks and text messages are secure; checks media files for malicious software and security threats; guards against phishing; and offers anti-theft protection. Lost or stolen smartphones can be found via Google Maps, plus you can turn your phone's GPS on remotely and have the device send its location to you. You can also lock your phone remotely.

Lookout protects iOS or Android devices from unsecure Wi-Fi networks, malicious apps, fraudulent links, etc. You can also use it to back up your contacts by scheduling automatic backups and then accessing the information online, or using it to restore your device in case of a crash or data loss. If you lose your phone, Lookout can locate it on Google Maps – even if the GPS is off and the phone is on silent.

For iOS, the Anti-Virus & Malware Scanner does much the same as AVG Mobilation but additionally lets you scan files on remote locations such as Dropbox and web servers. Trend Micro also offers good mobile security for Android.

- Put a security code on your smartphone in addition to the SIM code and engage the auto-locking feature.
- Disable network connections and switch off bridging connections. Do not broadcast the Bluetooth device name and disable automated peer-to-peer Wi-Fi connections.
- Turn off Geotagging and GPS location via *Settings*.
- Whenever possible, access 2G, 3G or 4G networks in preference to free Wi-Fi services.
- Do not store sensitive files on the phone's internal storage. Encrypt data onto the SD card or hide in a secret compartment.
- Enable remote-find or remote-wipe features.
- Do not 'Jailbreak' any device – the act of removing limitations through software or hardware exploits.
- Avoid connecting personal devices to the office network or computer.
- Watch for unauthorized charges, rapidly-depleting battery and unusual text messages.
- If you link your smartphone to your car's on-board computer, be sure to regularly delete sensitive information, contacts and travel history.
- Employ a mobile data backup service, such as Trend Micro.
- When covering demonstrations, etc, replace the SD card in the phone with a spare that does not contain personal data and contacts in case of arrest. Also, switch to Airplane Mode to avoid being tracked.

007 Apps

The smartphone in your pocket can easily be turned into a high-tech spy tool and counter-surveillance device to rival anything that Ian Fleming's Q might have dreamt up. You can secretly record, access banned content and communicate securely, particularly so if used with an unlocked phone and an unregistered pay-as-you-go sim card.

You can take your smartphone onto Tor and keep everything off-radar using apps for Android and iOS with access to both Deep and Surface Webs, plus PM and email without being monitored or blocked.

In certain situations, such as a demonstrations and riots, Tor-enabled mobiles can still connect to social networks and websites which may be blocked by the government. However, most social

networks make heavy use of JavaScript which will give your identity away but Twitter does have a mobile facility as does Facebook Mobile which do not use JavaScript and can, therefore, be accessed anonymously.

- **Scramble Calls** —Silent Phone for Android and iOS provides HD quality securely-encrypted phone/video communication over any network – 2G, 3G, 4G, WiFi. RedPhone offers end-to-end encryption for Android.
- **Secret Messenger** — there are secret messaging systems for all devices. Secret SMS for Android and iOS will encrypt messages between users and hide them. The iOS iMessage uses secure end-to-end encryption and "cannot be intercepted regardless of the cell phone service provider," according to a Drug Enforcement Agency internal memo.
- **Secret Image** — Secret Video Recorder Pro for Android and iOS allows you to seemingly switch off the smartphone while continuing to film. A quick examination of the phone will not show any activity. You can also make and receive calls while the camera is secretly running. Secret Camera for iOS allows you to take photos discretely with no shutter sound, preview or immediate playback, while the Mobile Hidden Camera does the same for Android. ReconBot for Android and iOS is a stealth video recorder that displays a black screen while it records. Includes remote view so you can watch the recording live via a web link. Also includes location data.
- **Remove Image Data** — if you want to upload images that cannot be traced back, you need to remove or alter the EXIF data which most modern cameras implant in the image to give GPS location and other details. Options for Android include the ExifEraser and ExifRemover for iOS. 'Geotagging' can be turned off in most Android and Apple mobile devices by going into the *Settings*.
- **Secret Audio** — there is Secret Audio Recording for Android and Spy Recorder for iOS which can also automatically record when you enter certain locations that you set with Google Maps. The Top Secret Audio Recorder for iOS is a covert recorder that looks like a regular picture-viewing app. You can swipe through the photos but as soon as you tap on an image the recording begins. The recordings can also be password protected.
- **Record Calls** — Top Secret Call Recorder for Android and Call Log Pro for iOS.
- **Confirm Contacts** — if you receive a call and want to know who actually called, add them to a *Contacts* file and check them out with Contact Spy for Android and iOS which lets you quickly search people or companies by running them through this search engine app for web entries, images, news, blogs and US-only physical addresses.
- **Secret Compartment** — secret folders for Android and iOS. Protect sensitive data by storing it in a hidden and encrypted file.
- **Location Trackers** — helpful for dangerous assignments, GPS tracking allows for real-time monitoring of a phone's location via Google Maps. Some, like GPS Tracking Pro for Android and iOS, have a check-in feature so you can let the office know you are okay. Also highlights nearby safety points like hospitals.
- **See in the Dark** — enhanced night vision photography and live feeds with the Night Vision Camera for Android and iOS. Works best on cameras with a good-quality lens.
- **Ranger Finder** — the iTelescope for iOS works to military specifications and integrates an accurate rangefinder, angular measure, altitude gauge, sextant and theodolite, electronic

viewfinder and night vision spyglass with GPS location. Will also encrypt captured images and data. Not available for Android, although there are lesser options.

- **Police Scanner** — there are several police and emergency service scanner apps. Police Scanner for Android taps into scanners from around the world. For iOS, Radio Police Scanner does much the same.
- **Track Planes** — Plane Finder – Live Flight Status Tracker for iOS and Android displays thousands of flights globally using real-time ADS-B signals used by aircraft to transmit their positional data. Enter flight number or tap on the map showing the planes above your head.
- **Chart Vessels** — monitor the position of all manner of vessels from passenger and cargo ships to yachts and gin-palaces. Ship Finder – Live Vessel Tracking for iOS and Android picks up AIS position data from around the world and provides details and photographs of the vessels.
- **Mobile VPN** — to cover your back, there is Hotspot Shield which encrypts all smartphone traffic through a Virtual Private Network (VPN) to mask your identity and prevent tracking (not recommended for use with Tor because it puts strain on the network). It also allows you to view banned content and access Twitter and Facebook mobile if their services are ever blocked locally.
- **Panic Button** — In The Clear is an Android app that securely wipes a phone of sensitive data at the click of a button.
- **Remove Evidence** — there are shredders for Android and iOS.
- **Self-Destruct** — perhaps the ultimate weapon in Q's arsenal is the self-destruct feature. For this the iOS has the edge with the free Wickr app which allows you to encrypt any data – text, pictures or videos – and then have them self-destruct once unscrambled and viewed, leaving no trace for the forensic investigator. An Android version is coming soon.

7. IP Cameras

Modern surveillance cameras use the same technology as any web-enabled device to stream video directly onto a network and, if you know the IP address, you can access the camera on a smartphone or any Internet computer.

Curiously, many cameras are not password-protected; this is especially true of those on private property which often provide street views. Some even have Pan Tilt Zoom functionality which allows anyone to zoom in and out and move the camera around.

To access a specific camera you need to know its IP address, which will look something like this http://50.37.237.4/. Here you can take control of a security camera at Boundary County Airport, Idaho. A quick Google search will provide live views of cities globally, or visit earthcam.com and control the cameras on Times Square and thousands of other locations.

For newsgathering, IP camera smartphone apps offer the ability for live visual contact and coverage of events. A reporter armed with a smartphone and webcam app like SpyWebCam Pro for Android or iWebcamera for iOS can stream a live feed which can then be monitored back at base or by others in the field with mLiveCams for Android or IPCamSoft for iOS.

An editor miles from the action can switch between cameras operated by the reporters, control public and private street cameras, watch multiple views and record video segments and stills and then upload or email them onwards. They can also speak directly with each reporter using the traditional telephone feature and control the action like a live TV director. To improve coverage, tether a wearable spy camera to the reporter's smartphone.

8. Keeping out the Spies

When it comes to securing your system, there are three main concerns – ad networks, cybercriminals and law enforcement – and they all use similar techniques. Generally, they do this by so-called "social engineering", the art of enticing users to malicious websites and then tricking them into giving out confidential information or by planting malware in their system there and then or via email.

At the basic level, ad networks do this whenever users take onboard cookies. Cybercriminals make the most of news events and consumer trends to draw people to a webpage where malware will automatically plant itself in the computer, known as a "drive-by download". Malware can also be surreptitiously planted in legitimate websites to infect even the wary. These are known as "watering hole" attacks.

Within hours of the Boston marathon bombing, the spammers were sending out emails and Twitter links seemingly from CNN which sent users to sites compromised by a Blackhole Exploit Kit where many were infected by Trojans, backdoors, infostealers or rootkits. The same thing happens around most major news stories. And it's not just the gullible public who fall prey. Seasoned journalists are regularly sucked in with the apparent deaths of celebrities or by looming sex scandals.

Another growing threat is Ransomware, which locks a computer until a "fine" is paid. Infections often come via legitimate but compromised websites and advertisements where hackers have managed to insert malicious coding. Victims suddenly find their screen frozen and a fake warning from the FBI or local law enforcement saying they have been downloading illegal content. Even more unnerving, the perpetrators occasionally include a mug shot from the victim's own webcam. This malware is extremely hard to remove and, needless to say, once a fine has been paid the machine stays locked.

Intelligence agencies and law enforcement also use malware, one example being FinSpy, which they send to people in spoof emails, allowing agents to take control of smartphones and computers, intercepting Skype calls, turning on web cameras and recording keystrokes. Researchers have found FinSpy running on 36 servers world-wide from Austria to Vietnam.

However, dodgy redirects and 'drive-bys' can be pre-empted with a good anti-virus program.

To avoid infection via email, disable HTML in your email program via the *Settings* tab. Look for and untick *Display attachments inline* or tick *View message body as...plain text*.

Never open attachments or click on links if you are unsure of their origin. If you must open a suspicious attachment, disconnect from the Internet first and run it through an anti-virus 'sandbox'.

Equally, be aware of social media posts with enticing links, many of which are often shortened so you don't know where you are heading. Short URLs can be enlarged at LongURL.org.

It is also prudent to secure your home and office wireless networks. The simplest solution is to change the administrator password for the wireless router. Hackers can look-up the manufacturer's default password and easily break in, intercepting all the data you send and receive.

When choosing a password, select a memorable phrase rather than an actual word that can be found in a dictionary. For example, I Like Lots Of Vinegar On My Fish And Chips can be written as ILLOVOMFAC. You could add to this numbers and non-alphanumeric characters and a mix of upper and lower case.

Use a combination of standalone security software with one firewall, one or two anti-virus programs, and one or two anti-spyware programs. Also consider using dedicated anti-Trojan software. Avoid running them all in 'real-time' to avoid software conflicts and, instead, regularly scan your computer and update frequently.

Recommended Free Programs

As a rule, free, open-source software is preferable to the paid-for variety because developers and others can have a good look inside for backdoors and other things that should not be there.

- Comodo Personal Firewall — free and paid-for versions of combined anti-virus and firewall programs. The firewall application uses Cloud-based data to analyze new programs and prevent attacks. It protects against viruses, Trojans, worms, hacker attacks and other threats.
- Lavasoft's Ad-Aware — free and paid-for versions. Provides core protection against Internet threats. Featuring real-time anti-malware protection, advanced Genocode detection technology, rootkit protection and scheduler.
- Spybot Search and Destroy — free, fully functioning privacy and anti-malware software. Immunize feature blocks a range of uninvited web-borne infections before they reach your computer. Also includes Hosts File which blocks adware servers from your computer and System Startup which lets you review which apps load when you start your computer. A shredder is also included.
- AVG Anti Rootkit — removes Rootkits, a malicious program somewhere between a virus and Trojan horse which opens your computer to external attack.
- Crap Cleaner — free system-optimization tool. It removes unused and temporary files, allowing the computer to run faster and more efficiently with more hard-disk space. The application cleans traces left by Windows, Internet Explorer and third-party applications.
- Avast Free Antivirus — full-featured software with the same antivirus and anti-spyware scanning engine used in Avast's premium products.
- AVG Anti-Virus Free Edition — probably best of the bunch when it comes to free anti-virus software.

With all these programs, be sure to check the *Settings* and turn off *automatic updating*. Manually update at regular intervals.

Cleaning Up

The Heidi Eraser is freeware that allows you to completely remove sensitive data from a Windows hard drive by overwriting it several times with carefully selected patterns. The *Erase Secure Move*

feature erases all traces after you move files from one place to another. Eraser can also be set to erase the Windows *pagefile* on *shutdown/restart* and it has the option of being added to your context menu, so when you right-click a file you can select *Erase*.

Erasing History

To erase your tracks in one go consider dedicated cleaning software like CCleaner. When choosing shredder software, select one that gives you the option to specify the number of times data is overwritten. A minimum of three 'passes' is recommended.

Alternative Software

Microsoft's own software leaks like a sieve and is best replaced with the open source variety. Avoid using Office, Outlook, Internet Explorer, and Windows Media Player as they collaborate with each other.

- Use Open Office Suite instead of MS Office (Word, Excel, etc). Always disable *auto-save* in the program options.
- Use VLC Media Player instead of Windows Media Player.
- Use Foxit PDF Reader instead of Adobe Acrobat Reader. Be sure to tick *Enable Safe Reading Mode*. And untick *Restore Last View Setting when Reopenin*g.

*

Share the Knowledge

All journalists in the 21st century should be awake to the dangers of the digital world.

Please recommend 'Deep Web for Journalists: Comms, Counter-Surveillance, Search' to a fellow journalist or download the unabridged edition containing additional chapters on Secure Anonymous Blogging, other Hidden Networks, etc, and Deep Search – mining the archives and databases of the Deep Web.

"Compelling reading for all journalists" – Jim Boumelha, President, International Federation of Journalists

About the Authors

Author: Alan Pearce is a journalist, broadcaster and author with over 30 years' experience. He has written for Time magazine, The Sunday Times, The Times, The Sunday Telegraph and others, in addition to Sky News and various BBC outlets. He was injured covering the fall of Kabul in 1996 while working as the BBC's Afghanistan Correspondent and is the author of "Dunkirk Spirit", "Whose Side Are They On?", "The Google Questions" and the best-selling "Playing It Safe".

*

Editor: Editor: Sarah Horner is a former foreign and war correspondent who spent more than seven years living in the Asia-Pacific region, including long stints in Afghanistan, Pakistan and Cambodia. She covered Afghanistan for the Economist Intelligence Unit from 1996-2003. Since 2004, she has worked in digital communications, managing tech projects for organizations such as the BBC, Westfield Shopping Centers, Save the Children and the Children's Commissioner for England. Sarah is currently a freelance writer/editor and project manager.

*

Special thanks to Ernest Sagaga, Head of Human Rights and Safety at the International Federation of Journalists, for his support, foresight and professionalism.

*

BACK TO TOP