# Journalism post-Snowden:
## *a simple guide to protecting your information & contacts*

[redacted]
[redacted]

# Contents

# Credits


AUTHORS:

**Vian Bakir**, Professor in Political Communication and Journalism at Bangor University, researches the security state and public accountability; deception in journalism; and digital surveillance/ sousveillance. Her books include: *Intelligence Elites & Public Accountability* (2018), *Torture, Intelligence & Sousveillance in the War on Terror* (2016 [2013]), and *Sousveillance, Media & Strategic Political Communication* (2010). Her recent work includes numerous submissions to the UK Parliament's Fake News Inquiry, and House of Lords Joint Commission on Human Rights.

**Dr Paul Lashmar,** Deputy Head of Journalism at City University, has worked as an investigative journalist for the *Observer*, the *Independent On Sunday*, and TV's *World in Action*, *Timewatch* and *Dispatches*. His subjects included terrorism, the secret state (including the Edward Snowden story), organised crime, and business fraud. He has won Reporter of the Year (with David Leigh) at the British Press Awards, His next book, *Spies, Spin and the Fourth Estate*, is to be published in 2019. He is a member of the National Union of Journalists (NUJ).



FUNDER:

The guide was enabled by a grant from Bangor University Impact Acceleration Account/ Economic & Social Research Council: *Intelligence Elites & Public Accountability – Enabling Journalists* (2018-19).

ACKNOWLEDGEMENTS:

Thanks to John Battle (ITN), Duncan Campbell, Matt Fowler, Bill Goodwin (*Computer Weekly*), Gill Phillips (*Guardian News and Media*), and Tom Sanderson (TCIJ), for their input to the report (though errors remain the authors' own). We have drawn on the previous Infosec document by Silkie Carlo and the late Arpen Kamphuis. We have worked in partnership with the NUJ Campaign Manager Sarah Kavanagh.


HONESTY BOX:

This full guide for NUJ members contains suggestions that would give insight on Information Security (InfoSec) generally and journalists' counter-measures in particular, to misguided law enforcement agencies and malevolent hackers, phishers, private security intelligence operators and worse. Please do not circulate the full version of this guide. While an abridged version is widely available, the full version is available only from behind the NUJ members-only section of the union's website.

NUJ ETHICS:

The NUJ code of conduct was first established in 1936 and it is the only ethical code for journalists written by journalists. The code is part of the union rules; members support the code and strive to adhere to its professional principles. The code states:

> *A journalist at all times upholds and defends the principle of media freedom, the right of freedom of expression and the right of the public to be informed.*

The code also compels journalists to do their 'utmost to correct harmful inaccuracies' and it repeatedly highlights the importance of the 'public interest'. Furthermore, it calls on journalists to protect the identity of their sources who supply material and information in confidence.

In addition to the code, the NUJ strongly believes that it is the duty of journalists to hold the powerful to account. This duty can involve gathering and obtaining information that can verify or refute allegations relating to dangers that threaten the public, abuses of power and/or serious crimes and misconduct.


Design www.ronandevlin.com

# Introduction

# Why Journalists Should Assess the Threat of Digital Surveillance

This guide is for members of the NUJ in the UK and Ireland and provides practical advice about how to protect your information and contacts. Journalists should be familiar with the dangers of digital attacks, including those through hacking, phishing, surveillance and seizure, and take steps to protect themselves, their sources and their journalism.

The guide is divided into two parts. Part I briefly explains why digital surveillance matters for journalists. It then offers practical guidance to assessing journalists' threat and risk levels, and suggests measures that they should take to protect their data. Part II delineates the changing legal situation. It outlines key laws deployed against journalists; the change of direction in media law; and the constant erosion of press freedom.

Most cybersecurity and journalism **protection guides** include pages of complex technical setting up instructions to protect the reader with cybersecurity programmes such as TOR, Tails or PrettyGoodPrivacy (PGP) that even the experts find daunting. These are exceptionally high security approaches that can be of value if you are carrying out investigations into governments or organisations that could have access to material obtained from police or intelligence surveillance. However, such approaches may be excessive for most stories about, for example, health, local government, and industry (other than military contractors or very large multi-nationals). Risk assessment and proportionality about protecting yourself will help.

In 2013, US National Security Agency (NSA) contractor, Edward Snowden, turned whistleblower. The revelations that followed his **release of documents** on global surveillance showed how powerful the eavesdropping intelligence agencies such as NSA, but also Government Communications HeadQuarters (GCHQ), now are. However, while the UK's signals intelligence agency, GCHQ, has multifaceted invasive means of surveilling journalists (as they have anyone), they do not have the resources to pursue journalists except in exceptional circumstances. The UK's leading investigative journalist on intelligence issues, Duncan Campbell, counsels that it is important to keep things in perspective: 'The impact of Snowden's revelations should not really, be overstated for journalism, because the most critical aspect relates to the conduct of the intelligence' (interview with Duncan Campbell, cited in Lashmar 2017, p.677). Indeed, only a relatively small number of journalists are likely to run up against surveillance by the 'Five Eyes' network (namely, US, UK, Canada, Australia and New Zealand electronic spy agencies).

*Risk assessment and proportionality about protecting yourself will help*

# What this Guide Is

This guide aims to help match the threat to the kind of journalism that you are likely to undertake, and then to advise on data protection. The first thing that we ask you to do is to assess your risk and be prepared.

**We have identified four risk levels (see Box 1):**

- **Risk Level One:** You are a journalist who does not tend to do investigations or have confidential sources.
- **Risk Level Two:** You are a journalist who covers a range of stories and have some sources you would like to keep confidential and you occasionally do some in depth or investigative stories.
- **Risk Level Three:** You are a journalist who undertakes serious investigative reporting. You are producing journalism that offends the rich and powerful.
- **Risk Level Four:** You are a high-level investigative journalist whose investigations may involve holding to account the intelligence and security services, or senior members of the government.

*In Part I of this guide, we expand on these risk levels and actions that you should take.*

This guide is about protecting data, and preventing data loss that might result in exposure of confidential sources.

The guide is mainly concerned with UK and Ireland-based reporting, and visits abroad to relatively safe environments. If you are considering working in a high-risk environment and are employed by a responsible news organisation, they will have advice and support structures in place. Beyond this, there are other sources of advice:

- **NUJ** members can ask the union to help them to secure appropriate training and support from media employers. This can be done through collective negotiations with employers or via individual representation and support. If you think you need training but are not getting it then contact the NUJ for advice and assistance.
  The union also has a health and safety committee and an ethics council that can offer expertise and guidance.
- If you are a freelance, we suggest you go to the **Rory Peck Trust website** where there is excellent information.
- The **International Federation of Journalists** has a website dedicated to the safety of journalists.

*This guide aims to help match the threat to the kind of journalism that you are likely to undertake, and then to advise on data protection.*

## **Box 1** Four levels of risk – which is yours?

| RISK LEVEL | TARGET | THREAT | REQUIRES |
|---|---|---|---|
| Level One - Basic | Computer, email and phone | Data loss through theft, or loss of equipment, or random hacking | Basic security measures. Always use strong passwords Select encryption for storage wherever provided. Protect devices from theft |
| Level Two - Medium | Computer, email and phone. Cloud data | Low level targeting hackers or criminals. Request for data by subject or target organisations. Action under RIPA to identify confidential sources. | Consider carefully whether email or telephone records could identify any vulnerable sources.<br>If so, use burner phones, and if need be, multiple burner phones.<br>Check physical security for your devices and computers at home and in office |
| Level Three - Investigative | Computer email and phone. Cloud data. Organisation email | Data loss through law enforcement or regulator action. This may be accompanied by legal action. Or high level hackers instructed by targets. Or targeted attempt to reveal your source. | Ensure updates and security patches are enabled and applied on all phones and computers<br>Consider second computer |
| Level Four - High level investigative | Computer and phone | Covert data capture by intelligence operatives or high quality hackers | Air gapped computers. USB based storage. Tor Tails. Care with behaviour and use of any trackable activities |

# What this Guide Is Not

This is not a guide on how to handle sources.
(The pastoral case of confidential sources is always a challenging task.)

Nor is this a legal guide for journalists. It refers to various laws that authorities may use to access your data and materials, but it is not definitive nor does it cover all the laws that might be used against journalists undertaking their work. We recommend that you are compliant under the General Data Protections Regulations (GDPR) as this is likely to become increasingly used (to bog you down) by the legal teams of those you target (see Part II).

# Part I

# *A Guide to Threats and Mapping Your Risk Levels*

# Big Picture Problems from Digital Mass Surveillance

In 2013, US National Security Agency (NSA) contractor, Edward Snowden, turned whistleblower. The revelations that followed his **release of documents** on global surveillance showed how powerful the eavesdropping intelligence agencies now are. As the leaked documents reveal, their unofficial motto is 'collect it all'. These revelations generated extensive media debate and concern from politicians, regulators and civil rights groups in multiple nations (Bakir 2018).

Despite this debate, the post-Snowden surveillance regime ended up becoming even more extensive in the UK, with the introduction of the Investigatory Powers Act 2016 (Bakir 2018). Among other things, this Act allows data to be acquired, stored and analysed in bulk; requires telecommunications providers to retain 'Internet connection records' (which websites were visited but not the particular pages and not the full browsing history) of every British citizen for 12 months; allows over 40 public bodies (including the police) to access this data stored; and allows intelligence agencies to hack devices, networks and servers.

Many countries have legal and oversight constraints on domestic surveillance by the state. These commonly include restrictions on the types of techniques a state can use to conduct surveillance, or on a state's ability to surveil its own citizens, residents or members of protected professions, e.g. journalists, lawyers and members of parliament (Privacy International 2018).

Such restrictions on domestic surveillance by power-holders are vitally important. Without these restrictions, the ability to watch back – to hold power (including surveillant power) to account – is compromised. Such '*sous*veillance' (that is, watching from below, or from a position of powerlessness) is compromised by widespread digital *sur*veillance (that is, watching from above, or from a position of power) in at least two ways (Bakir 2015, Mann and Ferenbok 2013). Firstly, widespread digital surveillance compromises journalists' sources. Indeed, in 2018, the European Court of Human Rights found that the UK's methods for bulk interception of online communications violated the right to privacy and the right to free expression due to 'insufficient safeguards' concerning confidential journalistic materials (Council of Europe, Human Rights Europe 2018). As Part II will show, stories continue to emerge about journalists being surveilled, most commonly by the police, compromising journalists' sources and information. Secondly, widespread digital surveillance compromises 'sousveillance' via so-called 'chilling effects' on populations, discussed below.

*…if people are subject to mass surveillance they are no longer able to express themselves freely.*

## 'Chilling Effects'

The chilling effect was formally recognised in December 2013, some six months after publication of the first Snowden leaks, as the United Nations (UN) General Assembly adopted a Resolution that ties the right to privacy to the right to freedom of expression: if people are subject to mass surveillance they are no longer able to express themselves freely.

Since Snowden's leaks, chilling effects have been revealed amongst the wider public in:
Page views of Wikipedia articles relating to terrorism (Penney 2016).
A decline in 'privacy-sensitive' search terms on Google that could get users (from 11 different countries including the USA) into trouble with the US government (Marthews and Tucker 2017).
Usage of Facebook. In an experiment involving a hypothetical news post on Facebook about US airstrikes against ISIS, most participants when primed of government surveillance significantly reduced the likelihood of speaking out in hostile environments. When people perceive that they are being monitored online, they readily express opinions when they are in the majority, but suppress them when they are in the minority (Stoycheff 2016).

**Chilling effects also operate on journalists. Since Snowden's leaks, they have been demonstrated in:**
Self-censorship of American writers (PEN 2013).
American journalists' behaviour: a December 2014 survey of 671 US investigative journalists found that surveillance concerns prevented 14% of them from pursuing a story or reaching out to a particular source (Pew Research Center 2015 p.2).

In December 2018 the writers' group Scottish Pen released a report that contained a survey of 118 Scotland based journalists and writers that made clear the impact of surveillance on chilling open discussion. One in five writers (22%) surveyed have avoided writing or speaking on a particular topic due to the perception of digital surveillance, with another 17% stating they have seriously considered it (39% total); 82% said that if they knew that the UK government had collected data about their Internet activity they would feel as though their personal privacy had been violated; and 28% have curtailed or avoided activities on social media, with another 13% stating they have seriously considered it (41% total) (Williams, McMenemy and Smith 2018).

Better protection of your information and contacts will help avoid your information and sources being compromised, and your story being 'chilled' As we will see in Part II, there have been major changes in the direction of attack that journalists come under from the law. It used to be that you had to demonstrate the truth of your story by retaining all the evidence. However, the focus has moved to public interest, and you now need to be able to demonstrate that your acquisition of information and its retention has a strong demonstrable public interest defence.

*Better protection of your information and contacts will help avoid your information and sources being compromised, and your story being 'chilled'*

# Threats to Working Journalists

*The rapidly emerging digital environment offers great opportunities for journalists to investigate and report information in the public interest. However, it also poses particular challenges regarding the privacy and safety of journalistic sources* (Lashmar 2017)

Protecting your data is important to journalists for a range of practical and ethical reasons. The greatest risk facing the working reporter is the loss or theft of your hardware and from random hacking and phishing. In most cases, the fact that you are a journalist will not be the reason for the attack, but the more sensitive your work is, so the threat of targeted attacks increases.

## Being Targeted by the British Police

For most journalists the greatest threat by the state to confidential sources and data does not come from the intelligence services monitoring your activities. Rather, the greatest threat comes from the police, possibly acting for MI5, but more likely conducting more routine investigations. This is not just a threat to investigative journalists, but can equally be a threat to local or regional journalists who senior officers think are talking off the record to police officers. In the current political climate the police feel emboldened to hunt down journalists' sources even for stories that do not concern national security. There is a portfolio of powers being used, and there have been recent indications of the police utilising legislation in new ways to force journalists to reveal their sources (see Part II). There is also willingness by UK law enforcement to intervene on behalf of security forces from other countries that are after journalists' data. These new developments are worrying. The government pays lip service to freedom of the press, yet they are prepared to see journalists arrested, the tools of their trade confiscated, and huge costs incurred by resource-poor media operations.

There are many examples of surveillance abuses by the police (see Box 2). It is worth noting that none of these cases of surveillance abuses should have been instigated. Their sole effect was to divert journalists from doing their jobs. When you are raided, all your information and contacts are available to the police, not just the material relating to the case. Often you cannot work. Under Operations Weeting and Elvenden, that followed the phone hacking scandal, some 67 journalists were arrested and/or charged between 2011 and 2016. The police also monitor some journalists.

*…none of these cases of surveillance abuses should have been instigated. Their sole effect was to divert journalists from doing their jobs.*

## **Box 2** Examples of Surveillance Abuses by Police

**In 2008, local press reporter Sally Murrer was accused of obtaining police information illegally. The Thames Valley police used Regulation of Investigatory Powers Act 2000 to obtain her materials and communications data. In a landmark ruling, Judge Richard Southwell said that any evidence gathered by police using the bug should be excluded under European laws that protected the rights of journalists and their sources. Murrer later said: 'I was treated like a terrorist. The things they were investigating were absolutely bread and butter local paper stuff.' The Thames Valley Police have never apologised to Murrer and refused to accept that it was in any way at fault in the way it treated her (Press Gazette 2016).**

**In 2008, National newspaper reporter Shiv Malik was ordered to hand the police some source materials relating to a book he was writing on terrorism. Greater Manchester Police had originally obtained a far-broader order that would have seriously undermined the ability of journalists to persuade contacts to speak out. A judicial review, which was supported financially by the NUJ and *Times Newspapers*, ruled that the original order was too broad in its scope. Under a revised order, Shiv Malik handed over some of his source material, but under far more defined terms and in a way that will enable him to protect confidential sources.**

**In June 2009 a Belfast journalist, Suzanne Breen, won the right to withhold material relating to the Real IRA from the police, as her source would be at risk if she handed over interview notes. She had faced up to five years in jail if the judge had found in favour of the Police Service of Northern Ireland (PSNI) to hand over her material. During the case a source close to the Republican dissident group had issued a warning that she could be killed if she cooperated in the PSNI investigation. There has been frequent conflict with the PSNI over issues of media freedom, especially in relation to the protection of sources. Demanding the handover of footage, that broadcast and not broadcasted, has posed a threat to reporters and photographers.**

**In 2011, the Metropolitan police tried to use the Official Secrets Act 1989 to force *Guardian* reporters to disclose their phone-hacking sources. Complaints from the NUJ, International Federation of Journalists (IFJ) and its European group, the Federation of European Journalists (EFJ) prompted the police to withdraw their attempt the same day.**

## Being Targeted by the British Police (Continued)

The threats to press freedom of the type listed in this guide are predominately a problem in the UK and reflect the prevalence of surveillance capability. The NUJ has campaigned against surveillance of journalists for many years. In 2008, NUJ members were encouraged to obtain data held about them by the authorities including the Metropolitan Police 'National Domestic Extremism and Disorder Intelligence Unit'. In November 2013 (following Snowden's leaks) the NUJ launched a campaign to find out about the monitoring and surveillance of journalists, and asked members to submit 'subject access requests' to find out what information was held about them. Six NUJ members, all of whom had worked on media reports that exposed corporate and state misconduct, found that their lawful journalistic and union activities were being monitored and recorded by the Metropolitan Police. In November 2014, they took legal action against the Metropolitan Police Commissioner and the Home Secretary to challenge this ongoing police surveillance.

As a result of the NUJ campaign, freelance video journalist Jason Parkinson returned home from holiday in 2014 to find a large envelope in his mailbox. When he opened the envelope, he found nine years of his life laid out in detail. Parkinson's documents were police intelligence logs recording which protests he covered, who he spoke to and what he wore. Parkinson's documents, obtained through a subject access request, are the basis of an ongoing lawsuit filed by the NUJ against London's Metropolitan Police and the Home Office.

The campaign helped prompt the Interception Commissioner to launch an inquiry which found police forces had used the Regulation of Investigatory Powers Act (RIPA) 2000 to secretly view the phone records of 82 journalists in order to identify their sources in a three-year period. Up to 2015 such requests had been signed off internally by police forces themselves. The Interception Commissioner found that forces had ignored considerations of Article 10 (freedom of expression) of the European Convention on Human Rights which give a high level of protection to journalists' sources under European law. The Commissioner then called for a change in the law to provide judicial oversight of telecoms requests to find journalists' sources.

Box 3 summarises recent rulings in the UK on police surveillance of journalists. By and large, at the time of writing, seizure of journalists' data and materials requires judicial approval, but a journalist or media organisation is not informed or able to challenge the application for this approval.

*…seizure of journalists' data and materials requires judicial approval, but a journalist or media organisation is not informed or able to challenge the application for this approval*

## Being Targeted by the British Police (Continued)

Such incursions on journalists' digital communications compromise the globally established ethical obligation upon journalists to avoid revealing the identity of their confidential sources. The issue of source protection has come to intersect with the issues of mass surveillance, targeted surveillance, data retention, the spill-over effects of anti-terrorism/national security legislation, and the role of third party internet companies known as 'intermediaries' (Lashmar 2017, p.18).

## **Box 3** Rulings on Police Surveillance of Journalists

**2012 'Plebgate'. The Investigatory Powers Tribunal ruled in December 2015 that the Metropolitan police broke the law when it secretly obtained the phone records of a reporter behind the 'Plebgate' exposé about an altercation between officers at Downing Street and the Tory MP Andrew Mitchell. The Investigatory Powers Tribunal concluded that the Met had breached reporter Craig Woodhouse's human rights and that of two other reporters, the political editor Tom Newton Dunn and reporter Anthony France, when it accessed their phone records in its pursuit of the Plebgate mole. However, while it found the police had unlawfully secretly accessed Woodhouse's phone records, they had acted in accordance with the law in relation to Newton Dunn, France and the Sun news desk. However, the tribunal refused to make a damages order against the Met (O'Carroll 2015, Ponsford 2016)**

**2015. Watchdog, the UK's Interception of Communications Commissioner's Office (IOCCO) said that the practice of retrieving journalists' data was being used by nearly half of all police forces, and without proper consideration of the fundamental principle of freedom of expression. A report by Sir Anthony May, the Commissioner, revealed that 608 applications, seeking data about suspected leaks to officials, had been authorised in 19 forces in the past three years. Police admitted snooping on communications between 82 journalists and 242 sources across 34 investigations (Rozenberg and Halliday 2015).**

**2016. The IOCCO found UK police snooped on journalists' sources without approval. It found four cases of police acquiring data to identify sources, including one deemed 'reckless' (Cox 2016).**

**2016. The Cleveland Chief Constable apologised in person to two regional journalists after his officers unlawfully eavesdropped on their phones. Iain Spittal announced a major overhaul of the force's Professional Standards. In December 2016 the Investigatory Powers Tribunal in London heard that the force used anti-terror legislation, the Regulation of Investigatory Powers Act 2000, to find out the source of damaging leaks. The force tracked the phones of *Northern Echo* journalists Graeme Hetherington and Julia Breen over months in 2012 – while she was on maternity leave – as well as those of other individuals (Media Lawyer Staff 2017).**

## The Laws that are Used

*There is recognition, but with limitations, that journalists should have the right to protect their sources*

There is now a portfolio of legislation that a variety of state intelligence and law enforcement agencies can use to access journalists' information and sources. They include the Police and Criminal Evidence Act (PACE) 1984, Regulation of Investigatory Powers Act (RIPA) 2000, Terrorism Act 2000, The Anti-Terrorism Crime & Security Act 2001, Serious Organised Crime & Police Act 2005, Investigatory Powers Act 2016, and more. There is recognition, but with limitations, that journalists should have the right to protect their sources. Contempt of Court Act 1981 s.10 protects the right not to disclose sources except in specific circumstances:

- Interests of national security;
- Interests of justice;
- For the prevention of crime;
- For the prevention of disorder etc.

The police have frequently used the Police and Criminal Evidence Act (PACE) 1984 to try to obtain documents and information from journalists. It requires the authorities to contact a journalist or media organisation before accessing their work (this is a 'production order', known as 'on notice'). This legislation enabled journalists and media organisations to challenge the request to access their footage, notebooks and other material/information in an open court. Using the Police and Criminal Evidence Act (PACE) 1984 legislation, in the past the NUJ has won significant legal victories to protect journalists' work, integrity and sources.

Before the Investigatory Powers Act (IPA) 2016 received royal assent, the NUJ, civil society representatives, politicians and media organisations worked together to campaign against the draconian proposals. As part of this work, the *Press Gazette*'s Save Our Sources campaign was launched in September 2014 after it was revealed that the Met Police had viewed the phone records of Sun political editor Tom Newton Dunn in order to find the police officers they believed had leaked information to the paper about the 'Plebgate' affair. The Investigatory Powers Act (IPA) 2016 gave the state unprecedented powers in national security cases. However, more generally they seem to be still using the provisions of Regulation of Investigatory Powers Act (RIPA) 2000 which was expected to be superseded by the Investigatory Powers Act (IPA) 2016.

In 2016, the government used changes in technology, including the increasing reliance and use of smartphones, as the basis to move away from the long-standing procedures and protections offered by the Police and Criminal Evidence Act (PACE) 1984. The authorities now have no obligation to contact a journalist or media organisation when they want to

access information and data stored on electronic devices.

## The Laws that are Used (Continued)

*…in some cases we are back to the journalist's basic deontological position: you have to be prepared to go to jail to protect your sources.*

In talks with the NUJ, UK government representatives have consistently claimed that information stored on electronic devices is owned by the communications provider (not the person who bought the device), and law enforcement agencies can now go to the companies to get this information in secret. The Investigatory Powers Act 2016 and the six related codes of practice provide the legislative framework and practical guidance to enable this to happen (Griffin 2016).

Even if you contain all your data in secure password protected storage that even the state cannot penetrate, your problems are not over. You could be forced to hand over your passwords or face jail. (This is an acute problem at the airport.) Journalists who keep their data secure, whether on computer, backup or the cloud, can find themselves instructed to hand over passwords. If you refuse, you face action under the Contempt of Court Act (CCA 1981). This Act allows courts to order that sources be revealed where it is in the interests of national security or justice, or for the prevention of crime or disorder. The courts have the right to strike 'a balance' in interpreting these criteria by referring to cases such as Secretary of State for Defence v Guardian Newspapers (1985) and Goodwin v The United Kingdom (1986), Camelot v Centaur (1998), Ashworth Hospital Authority v MGN Ltd (2002) and Mersey Care NHS Trust v Ackroyd (2007). There is a string of recent cases in the European Court of Human Rights (ECtHR), including Financial Times v UK (2009). Later, we consider some options, but in some cases we are back to the journalist's basic deontological position: you have to be prepared to go to jail to protect your sources.

# Mapping Your Risk Levels (1-4)

We encourage NUJ members (a.k.a. ethical journalists) to audit how you keep your data and, when engaged in a story, analyse the threat. This is essentially a balancing exercise between convenience versus redundancy versus security. This must be considered across all the various forms in which data are held and stored (Carlo and Kamphuis 2014).

**Journalists hold data in many forms:**

- Media: notebooks, recordings, photos, emails, paper documents, electronic files, address books, diaries, etc.
- Locations: desks, lockers, etc.
- Devices: work computers, home computers (and backups), smart phones, dictaphones, cameras, tablet notepad, USB sticks and external hard disks, etc.

**Journalists' phones, in particular, provide a range of vulnerabilities:**

- Automatic logging of your current/past locations;
- Automatic collection of metadata, i.e. the phone number and location of every caller; unique serial numbers of phones involved; time and duration of call; telephone calling card numbers;
- Theft and loss of data;
- Remotely accessing data when phone connects to public WiFi;
- Remotely accessing all data at any point the phone is on;
- Phone/voicemail tapping, intercepting, or recording;
- Covert remote automation of microphone to record audio;
- Covert remote automation of camera to capture images.

**Journalists also trust others to store their information securely:**

- Remote computers or data centres, Google Drive, Google Mail, cloud services such as iCloud, Dropbox, WeTransfer, etc.

**There are two key principles to bear in mind when auditing how you hold and store your data:**

1. Deleting data from a device or desktop does not usually remove or delete data, in memory.
2. Convenience vs. redundancy vs. security.

## **Box 4** Four levels of risk – which is yours?

| RISK LEVEL | TARGET | THREAT | REQUIRES |
|---|---|---|---|
| Level One - Basic | Computer, email and phone | Data loss through theft, or loss of equipment, or random hacking | Basic security measures. Always use strong passwords Select encryption for storage wherever provided. Protect devices from theft |
| Level Two - Medium | Computer, email and phone. Cloud data | Low level targeting hackers or criminals. Request for data by subject or target organisations. Action under RIPA to identify confidential sources. | Consider carefully whether email or telephone records could identify any vulnerable sources.<br>If so, use burner phones, and if need be, multiple burner phones.<br>Check physical security for your devices and computers at home and in office |
| Level Three - Investigative | Computer email and phone. Cloud data. Organisation email | Data loss through law enforcement or regulator action. This may be accompanied by legal action. Or high level hackers instructed by targets. Or targeted attempt to reveal your source. | Ensure updates and security patches are enabled and applied on all phones and computers<br>Consider second computer |
| Level Four - High level investigative | Computer and phone | Covert data capture by intelligence operatives or high quality hackers | Air gapped computers. USB based storage. Tor Tails. Care with behaviour and use of any trackable activities |

## Risk Level One

*Your biggest threats come from loss or theft of your hardware and from random hacking and phishing.*

You are a journalist who does not tend to do investigations or have confidential sources. Nonetheless, you have data on your computer, USB and phone that you need for your work, and some that you would not want other people to see. Your biggest threats come from loss or theft of your hardware and from random hacking and phishing.

The most straightforward basic thing to do is make sure that your phone and computer are both password protected with a strong password. You also have an obligation under data protection laws to keep any professional data secure.

## Passwords

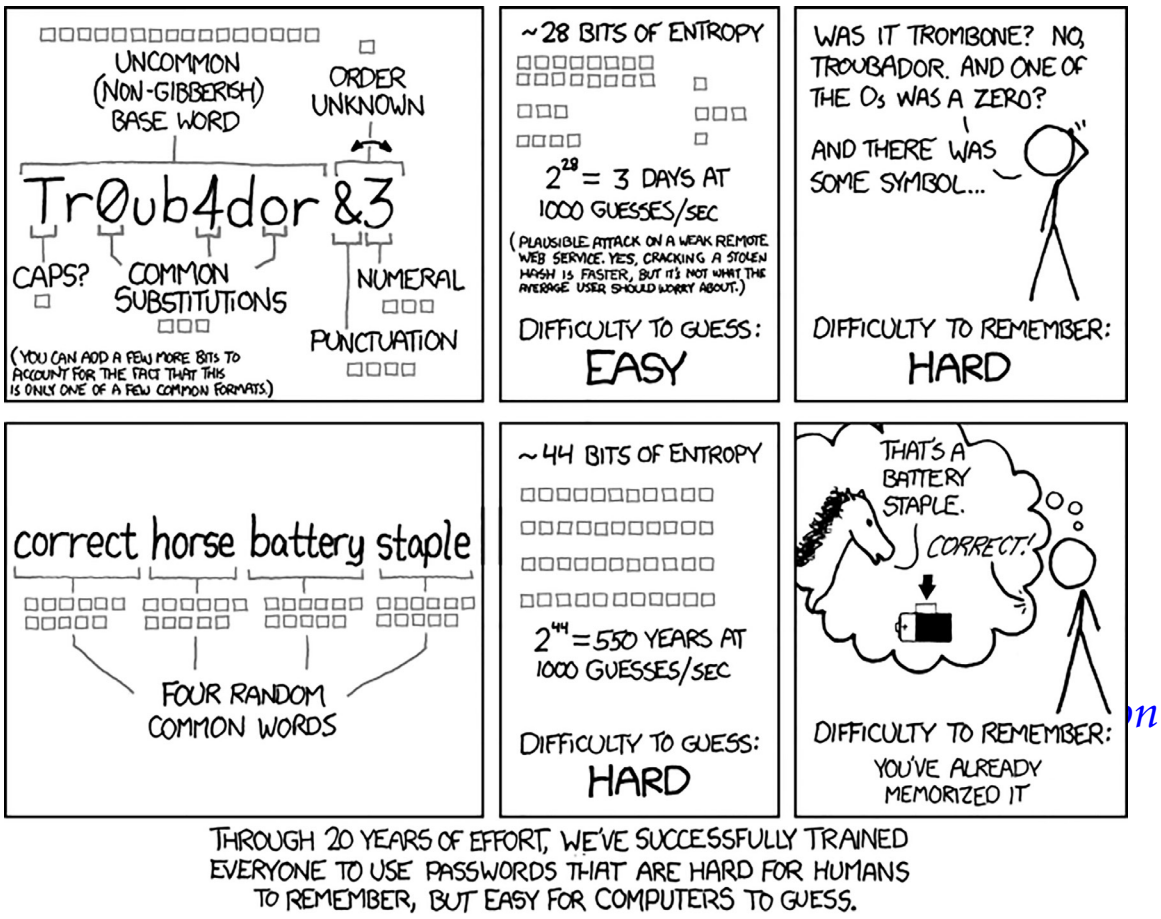
Managing passwords is now so complicated for all of us because we have dozens of devices, apps and online shopping sites that require us to have a password. It is not unusual to need access to 100 online and intranet sites that require passwords. All password advice says do not use obvious passwords like your offspring's names, dates of birth or the name of your pet. The big problem is remembering them all.

In using strong passwords, you are protecting against one of many ways in which your devices and online devices could be attacked.

Many sites, such as banks and government services, will insist that you use capital and lower case, and numbers, and perhaps special characters and a minimum number of characters. This is good advice to follow, but in fact not essential. An even simpler way is to use long strings of words from a sentence you know and remember.

One approach to creating a strong password is to use a memorable sentence.
An example from King James Bible (Matthew 7,6) is:
**'GiveNotThatWhichIsHolyUntoTheDogsNeitherCastYeYourPearlsBeforeSwine'.**
However, any book or newspaper cutting will do.

Another approach is to use four random common words, as illustrated below.




**(used under Creative Commons) See: https://xkcd.com/936/**

## Password managers

This is about the best way to keep passwords for multiple accounts: managers include 1Password, LastPass and Dashland. This protects your account even if someone has got hold of your password. Apps available in the Apple or Play stores will store collections of passwords securely. You can also simply use a quality encryption program to do this on a computer or any device. Use open source password management software such as KeePassX to generate a random, long, alphanumeric password (with symbols too, if they are permitted for the particular password), and then save it in your own encrypted password database. Turn on two-factor authentication (2FA).

## USBs

With the increased storage power of USBs, journalists may increasingly carry key data on a memory stick. They are very easy to lose. Most are not password protected. Use a data locker with a password: for instance, the Kingston DataTraveler Locker 64GB which costs just over £60. If you use Tails, you can keep your data in a password protected drive within the Tails OS essentially for free – the only cost is the USB stick, but you can use any generic USB stick above 8GB. This means you can have a fully password protected drive for less than £6 (Kingston have 32GB for £5.80).

## Storage

At this level if you are using Windows, depending on the Windows suite you have, there may be 'Bitlocker', an encryption system for keeping information securely. IOS devices have encryption turned on by default. MacOS has FileVault and on Android it can be found under device encryption.

## Two-factor authentication (2FA)

For the first three levels of risk assessment, an easy way of greatly improving login security is to use two-factor authentication (2FA). This works by requiring a second piece of information. You may be already familiar with the basic version of this process from online banking, where you transfer money and the bank sends you a passcode to reduce the chances of fraud. That's usually a temporary passcode delivered to your phone or device. It may also be something biometric, like your fingerprint.

It is worth switching on 2FA wherever you have the option as it can protect sites like your email, social media, Amazon, etc. Download an authenticator app, such as Authy, Google Authenticator or Duo Mobile. However, perhaps the best way to 2FA is to buy a security key - which is a USB device you can only use to authenticate into your account. They cost from £20 upwards. You set it up with your various accounts. From then on when prompted, rather than typing in a code, you just insert your security key and physically tap it during login.

Cyber-security reporter **Joseph Cox of Motherboard** says that hackers are starting to find their way round 2FA but it is still difficult. The hacker would have to be very experienced, determined and time rich so it really applies only to Level Four threats.

*If you once allow your private information to escape in the app ecosphere, you have lost all control*

## Contacts

Knowing how phone and email contact lists are managed and protected is critical to protecting sources. The problem is so severe that, unless you have, or can access, high technical skills, with Android and other devices you should maintain separate email accounts and phones for vulnerable contacts.

Typically, popular programs and applications will aggregate every new link you make or have via email or phone. Only with the most recent versions of Android has a user had the ability to turn off access to contacts, call and email records, documents or media on an app-by-app basis. This is welcome, and should be used robustly, but is also time consuming and has perils. Future app updates may attempt to restore denied access. Some companies, notably Facebook, have worked their way around protections, taking subscribers' contact lists and selling them to advertisers. Facebook have incurred massive fines, and face more - but it will happen again.

If you have ever installed Facebook, Instagram, Linkedin, and many more apps, they have probably asked for your contact list to 'improve your network'. Most readers have probably allowed their contacts lists to be lifted. If you once allow your private information to escape in the app ecosphere, you have lost all control. If that includes links to identifiable contacts, email addresses or phone numbers, you may have casually comprised your sources. If you make or receive a call on a smart phone with Facebook or similar apps running, it's likely that the fact of your link may be compromised. Consider an audit of your contacts lists.

## Emails

Most of us conduct our routine correspondence by email. Hotmail, Gmail and similar US providers all require the right to scan the contents of your emails as well as to store and trade your contacts. Use only European based email providers, such as the free or paid for email services from GMX, a German company operating in better data protection environment.

## Hacking and Phishing

Everyone is now a target for malware that damages your computer and phishing. If a phishing attack succeeds against you, like anyone else, you may completely lose control of your computer and devices to an unknown remote attacker, who may also offer the access for sale on bulk 'dark net' personal data marts. If you are lucky, you will only face unwanted extra advertisements and spam.

The most important rule is never (as in *NEVER*, *EVER*) click on a browser link in any email that does not come from a person you know and trust, and there is a reasonable clear purpose for the link.

Mouse or cursor over the link and see what site it will take you too. If it's a shortened link (like goo.gl or t.co, with a jumble of numbers and letters), mail your correspondent back for details and a direct link. Data thieves are getting better at targeting with convincing stories that could persuade you to hand over information.

## Anti-Virus

Use a trustworthy and well-reviewed anti-virus programme. Kaspersky, Bitdefender, and Avast are currently the three best rated free antivirus programs. However, US and GCHQ security experts are wary of Kaspersky, and believe it has been used by Russia as a mechanism for accessing private documents. It would be imprudent to rely on Kaspersky for investigating sensitive Russian stories, such as sports doping or the activities of oligarchs (Goodwin 2018b).

Tom Sanderson of TCIJ recommends installing the free version of **Malwarebytes** - not as a replacement for anti-virus, but as a second layer of protection and a cleaning tool.

When uploading free anti-virus programs, use custom install options to reject extra offers that you do not need. This is extra 'Bloatware' software that has unnecessary features that may use large amounts of your memory space. Install the minimum amount of software and extensions. Each extra piece of software can leave your system vulnerable. Some experts say that PDF readers and business software suites are particularly vulnerable. We have come to take lots of 'security' programs for granted.

## Social Media

If you are worried that the techno giants are extracting data that you would rather not have extracted from your postings, but don't have the time to research changing your settings, have a look at the **article** from The Washington Post (2018b).

## Different Operating Systems (OS)

Most NUJ members will use PCs or laptops using Windows Operating System (OS). Others might use Mac with an OS like Leopard. Techno savvy journalists might choose to use Linux the non-proprietary open source operating system. This influences some of the decisions you need to make along the way. Most viruses are targeted at Microsoft users. Mac viruses and Trojans do exist and are a potential risk, though there are not as many out there are there are for PCs.

# *It is worth auditing your backups. Where are they?*

## Backing up your devices

Anybody with any sense backs up their data from time to time, and on a separate hard drive or USB to the device holding the data that you are backing up. A lot of backups now are on the cloud. If the police coming knocking on your door with a warrant for your data, you want might want to make sure it is protected from seizure. It is worth auditing your backups. Where are they? If you have a lot of old data discs or external hard drives containing journalism material, not only are they a risk, but with archiving old data on, you may be vulnerable to issues under the new General Data Protection Regulations.

But where should you keep back-ups? Do you have external drives full of old back-ups stacked somewhere in the house? Ask yourself – what if the police raided your house and took that material? Is there information on there that could embarrass yourself or other people if made public? Is it password protected? Are you compliant with GDPR? One simple method is to keep backups safe and securely elsewhere, locked up so only you can access them, perhaps in the home of a close friend or relative who is not associated with your journalism.

It is useful if you are a data controller to have a GDPR plan which shows your approach to dealing with data - a 'weeding plan' to eliminate data when it is no longer needed for journalistic purposes. It would be good to keep a note as to why you are holding onto data after publication: for instance, after the year when libel and defamation cases are unlikely to occur.

## What if you have lost your hardware?

Android phones and iPhones have 'Find My Phone' features which can be useful if you mislay you phone, or if it is stolen (and kept switched on). It might also tell you to within a few metres where it is if someone has stolen it. Unfortunately, in the UK the police are overstretched and often reluctant to visit phone thieves. In order to get back your hardware if lost or stolen, or at least to recover your data remotely and then delete it, you can download an application called **Prey**. This is tracking software that helps users find, lock and recover their computers. You can activate the webcam to take a photo of its unauthorised user. It has several levels of service from free to $15 a month.

## Disposing of devices

In the case of phones, Apple and some Android manufacturers make changing phones and transferring data across easy. Part of the process is taking out the SIM card from the old phone and factory resetting to delete all your old data.

With computers, if you have had any confidential information of a personal or journalistic nature, and saved passwords on your computer, ideally you need to destroy the hard disc. Use a data wipe programme across your storage hard drive. Experts say it is worth three runs to clear all data and the process can take some hours. The programme BCWipe is a good as any. BCWipe Total WipeOut is a proprietary data erasure offering developed by Jetico, which boasts that its solution has been used by the Department of Defense in America along with the top 10 US defence contractors and national laboratories for 'military-grade' disk wiping.

## Risk Level Two

If you are at Risk Level Two, you are a journalist who covers a range of stories and have some sources you would like to keep confidential and you occasionally do some in depth or investigative stories.

As with Level One, your biggest threats come from loss or theft of your hardware and from random hacking and phishing. While you might take those Level One observations on board, you are also more likely to find yourself at the end of a directed attack. It may be that you are reporting on a criminal or rogue business person, and they might to want to know what information you have and whom your source is, so they pay a hacker to get into your devices. They might hack your emails. In addition, you may be writing about issues that attract people who dislike your viewpoint and seek to disrupt your life by stealing your data. You do not have to be Hilary Clinton to have your personal emails stolen and made public. Even those people who live the most squeaky-clean of lives have something we do not want made public (McStay 2017). Therefore, a rigorous approach to security is necessary.

### Box 5 Encryption

Encryption translates data into another form, or code, so that only people with access to a private key (often called a decryption key) or password can read it. Encrypted data is referred to as ciphertext, while unencrypted data is called plaintext. Encryption is one of the most popular and effective data security methods used by organisations. Two main types of data encryption exist - asymmetric encryption, also known as public-key encryption, and symmetric encryption.

### Emails

At this level you would still probably not consider going behind TOR or using a VPN system. When talking about encrypted e-mail companies, an important factor is where they are based and thus the data seizure laws that they are under the jurisdiction of. We have already mentioned GMX, a German company, but there is also ProtonMail based in Switzerland, and Hushmail, which encrypts email and is domiciled in Canada. One of the authors used Hushmail in the early 2000s but found that few other people did, therefore it was of little benefit. However, it now claims a range of developments, and the recipient does not have to have Hushmail. For a personal account they charge (at the time of writing) $32.98 per annum. It is used a lot for patient confidentiality in the US healthcare sector. Hushmail for iPhone offers encryption of your email whether the recipient uses Hushmail or not. The data is encrypted before it leaves your device, providing security to the body of your emails and attachments. The app supports two-step verification, Touch ID, and multiple accounts and aliases, and it is fully synced with your webmail account, for seamless access to contacts and settings. It is worth noting that these email systems are browser based and do not download to Outlook.

*Most browsers collect vast amounts of data about their users, which are often made available for marketing, intelligence agencies, and other nefarious purposes.*

## Browsing

There are serious privacy issues with our web browsing. Most browsers collect vast amounts of data about their users, which are often made available for marketing, intelligence agencies, and other nefarious purposes.

As detailed below there has been a big shift in the angle of attack against journalists by lawyers acting for the kind of people you might target. Changes over libel and defamation legislation have made it less attractive to go after journalists on these grounds. The new approach for disrupting inquiries is for lawyers to look for 'fishing' intrusions in personal and commercial privacy, and demanding a public interest justification. They are looking for any 'breach' that enables them to bog down the journalists and their news organisations. They will be interested in your browsing and search history in order to suggest that you were fishing or seeking to intrude on privacy. It is therefore wise to avoid any such claims, should you be required to produce your browsing and search histories. One method is to use a computer that is not linked to the searcher (you).

Although there are privacy issues with internet browsers, most of us choose a browser based on what we perceive as its usability, without taking privacy into consideration. However, you can improve your browser's privacy and security by adding 'extensions' – extra software that improves the functionality of your browser. Recommendations include HTTPS Everywhere and Disconnect. Carlo and Kamphuis recommended Firefox as a general purpose web browser for Linux and Windows. Chromium is a general purpose web browser for Mac.

## URL Previews

URL previews are a nice feature found in most messaging applications. However, when you browse to a website, your public IP address is exposed. This is just how the Internet works unless you are using Tor or a Virtual Private Network (VPN) to hide it. The difference with URL previews in messaging applications is that you are broadcasting to the website owner that you are discussing the website, as opposed to just browsing to it. If you are investigating the website owners, then that is a giveaway. For a clear discussion about this issue, see Seitz (2019).

## Virtual Private Network (VPN)

A Virtual Private Network (VPN) is a connection method used to add security and privacy to private and public networks including the Internet. VPNs are most often used by corporations to protect sensitive data. Using a personal VPN is popular with some investigative journalists and activists. If abroad somewhere dodgy, it gives you a secure tunnel home: the locals can see nothing of your activity. VPNs have been used for communicating in China to avoid the rigorous censorship and surveillance (although the Chinese government has been cracking down).

Privacy is increased with a VPN because the user's initial IP address is replaced with one from the VPN provider. Subscribers can obtain an IP address from any gateway city that the VPN service provides. For instance, you may live in London, but with a VPN, you can appear to live in Amsterdam, New York, or any number of gateway cities. A useful analogy of what a VPN does is that a firewall protects your data while on the computer and a VPN protects your data on the web. With VPNs you can:

- **Hide your real IP address;**
- **Change your IP address;**
- **Encrypt data transfers over public WiFi;**
- **Mask your location by choosing the country of origin for your Internet connection;**
- **Access websites blocked by governments.**

There are many VPN providers, some of which offer a free service. Paid VPN providers tend to offer robust gateways, proven security, free software, and unmatched speed.

## Encrypted Calls

Even at Level Two you might need to have phone conversations that cannot be hacked and are entirely private. In this case you need the Signal app (there are other similar apps), as does the person you are calling. Signal is an encrypted communications app for Android and iOS and a desktop version is available for Linux, Windows and MacOS. It uses the Internet to send one-to-one and group messages, which can include files, voice notes, images and videos, and make one-to-one voice and video calls. Signal uses end-to-end encryption to secure all communications to other Signal users. The applications include mechanisms by which users can independently verify the identity of their messaging correspondents and the integrity of the data channel. The Android version of Signal can optionally also function as an SMS app.

*…among Snowden's revelations are details of the NSA's ability to intercept and store Skype communications. We should assume that all Skype communications are not just between our contacts and us but with intelligence agencies too.*

### Voice over Internet Protocol (VoIP)

Voice over Internet Protocol (VoIP) software provides voice and video calling over the Internet, such as Skype and FaceTime, and is very popular with journalists. As of 2017, Skype had over 300 million monthly users. However, among Snowden's revelations are details of the NSA's ability to intercept and store Skype communications. We should assume that all Skype communications are not just between our contacts and us but with intelligence agencies too.

Some experts say Facetime is more secure in that, being an Apple device, it has end-to-end encryption: however, as the code is proprietary, it has not been independently audited in any way. Whatsapp is also end-to-end encrypted and has VoIP functionality (although it, too, is proprietary and is owned by Facebook). Signal now has decent, user-friendly end-to-end encrypted VoIP functionality. It is both open-source (and the code is therefore open to independent audit) and is owned by the non-profit Signal Foundation. Tom Sanderson recommended this for most journalists if they feel they need to use VoIP.

### Travelling abroad

Even at Risk Level Two, having a second computer and phone is useful if you travel abroad. An increasing number of countries have laws that require you to hand over your passwords so that they can download and inspect your data. In some cases, countries can suck up your data at ports of entry without your realising it. NUJ members have reported problems at airports when the authorities have asked for access to computers and phones. Therefore, the best thing is to have a computer and phone that has minimal, non-incriminating data installed. This will allow you to work in the usual ways (email, word process, search) but without incriminating any sources.

In October, 2018 the UK's independent reviewer of terrorism legislation called for greater clarity over the use of Schedule 7 stops, which allow police to question people and copy data from their mobile phones and computers at ports and airports without reason for suspicion. As Goodwin (2018a) notes, this has caused controversy, particularly among Muslims, who argue that they are singled out disproportionately for questioning when they travel abroad. Indeed, this fact is borne out by government statistics. Max Hill, the director of public prosecutions, states that he had concerns about the measures and would like to see 'a bigger, meatier code of practice' in place (Goodwin 2018a).

*…the best thing is to have a computer and phone that has minimal, non-incriminating data installed. This will allow you to work in the usual ways (email, word process, search) but without incriminating any sources.*

## Buying a second laptop and phone

Buy your second computer or second 'burner' phone using cash and not revealing your identity. A burner phone is a cheap, cash-bought, throwaway, low-tech phone, with a prepaid SIM card not registered to your person, to be used only for specific journalistic purposes. Using a dumb phone, for example the Nokia 3310, will help considerably because it does not run apps. A Nokia 105 is cheaper and goes further - it has no internet connectivity, so the hackers and data thieves have nothing to work with. It costs £15 at the time of writing. A stock of Nokia 105s or similar, and Pay-as-You Go SIM cards, is the ideal combination for 'burner' phones. One such phone is likely to be enough, unless your investigation is in a category requiring higher security. It can be hard, in some countries, to buy a SIM card without registering it to your personal details. Therefore, buying second-hand, or having a contact who can obtain such SIM cards, is ideal.

If the phone becomes associated with you and attracts surveillance, you should destroy it and use a new one. Changing the SIM card is not sufficient, as each phone handset also has an International Mobile Equipment Identity (IMEI) number that identifies the phone.

Intel started to put special components in their chipsets (combinations of chips that work together on laptop motherboards, i.e. the 'computer' within the casing) to allow automated management of systems over a network. This is called 'Intel Advanced Management Technology', and means that an I.T. technician in a large office can update software, or do other things to machines, without having to be physically near them. Unfortunately, the same functionality can be abused to install spyware or manipulate the systems in other ways. All laptops made after 2008 contain these chipsets, and are therefore vulnerable to these types of attacks when they are on a network (e.g. the internet). It is thought that the 'Intel 945' chipset is the most recently made chipset without this automatable feature, and hence lends itself to a securable motherboard (Carlo and Kamphuis 2014).

*Police forces have learnt a lot about accessing and controlling computers remotely. They now have the capability to access hardware and enter software without the user being aware.*

## Buying a second laptop and phone (continued)

Police forces have learnt a lot about accessing and controlling computers remotely. They now have the capability to access hardware and enter software without the user being aware. They have developed this to tackle criminals and pedophiles, but it is perfectly possible that with the right warrant, they can target you. If you are not connected to the Internet then you cannot be accessed.

Many security-minded users are now paranoid about other people accessing their computers remotely. They suggest putting tape over the webcam so you cannot be filmed remotely. Although it is unlikely that most people will be targeted by unauthorised remote use of their webcam, it is also one of the simplest, cheapest and least inconvenient security fixes possible. We recommend everyone (especially journalists) puts a small sticker or piece of tape over their webcam when not in use as the cost and inconvenience is negligible and it does fix verified security vulnerability, even if the risk is minimal.

The advantage of the old computers like the IBM pre-2009 was that you could open them and physically cut the microphone cord. More computer savvy users can, in some cases disable the webcam and microphone in the BIOS of the computer. The BIOS (Basic Input/Output System) is the program a personal computer's microprocessor uses to get the computer system started after you turn it on. It also manages data flow between the computer's Operating System and attached devices such as the hard disk, video adapter, keyboard, mouse and printer.

## Disposing of old equipment

At this level you might have confidential information on your mobile device and when disposing of it, the re-set function is not enough. These devices are tricky and there are plenty of apps that say they can do the job. One simple method, where the mobile supports it, is to encrypt the internal storage before triggering a factory reset. Some experts suggest filling the phone with dummy data before repeating the process. As for microSD cards, the best option is to take them out of the device and use a PC utility to wipe them.

## Risk Level Three

Risk Level Three is where you are a journalist who undertakes serious investigative reporting. You are producing journalism that offends the rich and powerful. These are people with money, and can hire lawyers, private investigators or high quality hackers to find out what you are up to. This guide does not propose to give a detailed account of how to align your hardware and software so that it is not vulnerable if you are doing this work. We are just going to suggest some key areas to consider.

Certainly at this level it is seriously worth considering whether you should have two laptops and phones. One would be for your standard work and the other for more difficult investigations. There are different ways of doing this. It may be a computer that you never connect online and you keep very secure. This is known as 'air-gapped'. It might be a computer that you have no data on and only use when you attach a USB. You should also think carefully about attaching a printer (printers can also retain information) and avoid printing out too many hard copies. You can consider encrypting and hiding data on the USB or HDD through software like Veracrypt that can also create encrypted and hidden folders on hard-drives as well. Your second computer may be completely designed and programmed to be secure. You should make all your security arrangements before using it.

The internal components that could potentially be used to surveil you, your source and your work are: webcam, microphone, hard disk drive, Wi--Fi card, Bluetooth card, 3G modem, Ethernet port, extra storage card, BIOS and Chipset (post Intel 945).

### Emails

We have already seen what ProtonMail and Hushmail can do. The higher level is using the email system in Tails, which in turn, relies on Tor. The next section explains what Tor and Tails do.

*Risk Level Three is where you are a journalist who undertakes serious investigative reporting. You are producing journalism that offends the rich and powerful.*

## Tor

Tor ('The Onion Router') is an open network that helps defend against 'traffic analysis', the network surveillance that challenges personal freedom and privacy, confidential business activities and relationships, and state security. Tor protects you by bouncing your communications around a network of relays all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location. The Tor browser was especially designed for anonymity by routing all of its traffic through the Tor network. This is a global network of computers called Tor nodes that have encrypted connections with each other. When the Tor browser starts, it will connect to one of these nodes. This node will connect to a second node that will in turn connect to a third node. All these nodes can be anywhere in the world and the first and third node will not be aware of each other. The third node will connect to the wider Internet and fetch webpages from the sites you are visiting. Those sites will not be able to see where you are or who you are (as long as you do not identify yourself by logging into services associated with your real identity).

In order to ensure the safety of the browser, Tor automatically enables https and automatically avoids extensions such as Flash, Realplayer and Quicktime that could undermine the process.

If the network provider you are using (this may be the entire country or just a university network) blocks access to the Tor network, you can use 'bridges' to achieve access. Bridges are Tor relays (nodes or computer points that receive traffic on the Tor network and pass it along) that help circumvent censorship. Using Tor you can:

- Be anonymous online by hiding your location;
- Connect to services that would be censored otherwise;
- Resist attacks that block the usage of Tor using circumvention tools such as bridges.

To learn more about Tor, see the official **Tor website**.

*Tor ('The Onion Router') is an open network that helps defend against 'traffic analysis', the network surveillance that challenges personal freedom and privacy, confidential business activities and relationships, and state security.*

## Tails

If you want a built-in encrypted email and chat. Tails is a live system that aims to preserve your privacy and anonymity. It helps you to use the Internet anonymously and circumvent censorship almost anywhere you go and on any computer but leaving no trace unless you instruct it explicitly to do so. Tails offers in-built encrypted and private messaging. Tails includes Thunderbird (Mozilla's email client) and uses the Enigmail extension for Thunderbird to handle OpenPGP encryption. It is a complete Operating System designed to be used from a USB stick or a DVD independently of the computer's original operating system. It is **Free Software** and based on **Debian GNU/Linux**.

Tails comes with several built-in applications pre-configured with security in mind: web browser, instant messaging client, email client, office suite, image and sound editor, etc. You cannot encrypt or decrypt mail in your web browser (unless you are using the Tails operating system).

Tails relies on the Tor anonymity network to protect your privacy online: all software is configured to connect to the Internet through Tor. If an application tries to connect to the Internet directly, the connection is automatically blocked for security. You can boot Tails from USB so it does not save changes to OS after shutdown and stores nothing on HDD. To find out more about how Tails ensures that all its network connections use Tor, see the Tails site **design document**.

## Passwords

Bear in mind that password protection for hard drives does not protect hard drive data, only booting into the operating system itself. Retrieving your data is as simple as plugging that hard drive into another computer to access the data on it. Most Linux distributions (including Debian) offer encrypting the boot drive or home folder during installation. The OS will then ask for an encryption password when the computer is booted up in order to decrypt the whole boot drive.

## Browsing

Use a general purpose browser with privacy-enhancing extensions for daily activities, but at Risk Level Three you might want to consider Tor as a secure browser that anonymises your location and identity. There no point in using Tor for sites that you are logging into with your real identity, unless your main concern is to hide your location. Remember to clear your Internet browsing history.

## Second computer and phone

Using a second computer at this level for your secure work probably means that you will need advice from one of the journalists' groups that specialise in cybersecurity.

## Risk Level Four

You are a high-level investigative journalist whose investigations may involve holding to account the intelligence and security services, or senior members of the government. You may be investigating offshore jurisdictions, powerful multinationals and rogue governments elsewhere. You fall into the category that Duncan Campbell would suggest also most certainly attracts the attention of either government or private intelligence agencies of the highest order.

The Snowden leaks revealed how extensive and powerful the surveillance capability was of the 'Five Eyes' network (plus its 39 additional partners). However, the most recent documents are over six years old. You can be sure that GCHQ, and its allies have moved on a long way in surveillance with the massive resources they have available.

At Risk Level Four, with relatively few journalists operating, each individual handles their security to the best of their ability. It is likely that if you are in this category, you already are well informed about security measures and use them. There are other detailed documents about security. We include some of the basics here for people who are interested in, or might be moving into, this level of investigative journalism.

### Mobile phones

Carlo and Kamphuis (2014) make the point that at a high-risk level, a phone basically is your adversary. At the very least, it can lock onto your location. You can turn off locations services but it still knows the nearest mast you are transmitting to. All associated metadata with the device is in the hands of a Five Eyes intelligence agency. At worst, it can be used to covertly collect the content of all of your phone calls, let alone all other data on the phone, and can covertly automate your microphone and camera to record audio and images (if it has a camera) too. This type of phone surveillance is very easy and basically comes at zero-cost to Five Eyes intelligence agencies. At this level, burner phones are the only serious InfoSec action for phone communications.

*You are a high-level investigative journalist whose investigations may involve holding to account the intelligence and security services, or senior members of the government.*

## Operating Systems (OS)

Popular Operating Systems include versions of Windows (e.g. XP, Vista, 8), OS X (for Mac), and Linux. Unfortunately, we know that intelligence agencies hide 'backdoors' in popular Operating Systems to enable covert access to users' data.

Linux is the leading open source, community developed, Operating System. There are many different versions of Linux Operating Systems that you can use. Ubuntu is the most widely used. It is easy to install, highly functional, and user friendly (but it is not advisable to use on Macs). You can replace your Windows Operating System with Ubuntu, or you can run both Windows and Ubuntu on the same laptop (which may help familiarise users with the new system before they commit). However, some knowledgeable experts recommend Debian over Ubuntu. Debian is more stable as it is not as regularly changed, limiting potential security and software flaws. Running Linux does require some computer science skills.

## SecureDrop

SecureDrop is an open-source software platform for secure communication between journalists and sources (whistleblowers). SecureDrop uses the anonymity network Tor to facilitate communication between whistleblowers, journalists and news organisations. SecureDrop sites are therefore only accessible as hidden services in the Tor network. After a user visits a SecureDrop website, they are given a randomly generated code name. This code name is used to send information to a particular author or editor via uploading. However, Carlo and Kamphuis warn that setting up such systems properly and keeping them secure is not a trivial matter. It should not be done without involving specialists with a proven track record, and it is not a realistic solution for an independent investigative journalist.

## Emails

It would be a good idea to have an anonymised email system so your emails cannot be read by anyone. As far as we know TOR/TAILS has not been broken and probably will not be.

## PrettyGoodPrivacy (PGP)

Many full time investigative journalists use PrettyGoodPrivacy (PGP), an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. PGP does not protect metadata – so although the contents of an email may be protected, the fact that you have sent an encrypted email to a particular contact will be known to the intelligence agencies.

It enables investigative journalists to receive information over the internet from known or unknown sources. These journalists put their PGP keys on their online details.

# **Box 6** What is PGP?

All email communication should be viewed as analogous to postcards, in that any message sent through electronic means is entirely open to be read by anyone who intercepts the message. Within this analogy, encryption is the equivalent of placing your message into a sealed envelope, making it much more difficult for anyone but the intended recipient to read the content of the communication.

The vast majority of email is encrypted to some extent, but the encryption offered by Gmail or Outlook is all handled by the email provider (Google, Microsoft, etc.) and they will generally have a quick look at each 'postcard' that comes through their mail depot, for reasons of your convenience - so they can check for spam, phishing scams or offer auto-reply suggestions, for instance.

For most purposes this is secure enough, but when you're sending or receiving sensitive information, especially in a journalistic capacity, it's worth considering taking responsibility for encryption into your own hands. This is where PGP comes in and if you use a plug-in or extension (and with a bit of getting used to) it's not as technically complicated as you might think. Many people use Thunderbird (Mozilla's email client, through which you can access a Gmail or Outlook account) and a Thunderbird plugin called Enigmail, which handles the PGP encryption.

Essentially, PGP provides you with a lockable 'envelope' for each 'postcard' you send. However, these 'envelopes' have one key for locking them and a different key for unlocking them. The key for locking (or encrypting) the message is your public PGP key and anyone who wants to send you a locked message will need a copy of this key. So we make infinite copies of this key (the public PGP key) and make it as easy as possible for people to get hold of a copy. Many people put their public key on a personal website from which people can quickly and easily download a copy. There are also publicly hosted 'keyservers' that keep libraries of public keys and can be searched for the email account that you want to send an encrypted email to. It is also very easy (using Enigmail/Thunderbird) to attach a copy of your public PGP key to an email that you send to a contact, so that they can encrypt their reply to you.

The other key (your private PGP key) is the only one that can unlock 'envelopes' that have been locked with a copy of your public PGP key. You should have only one copy of this key (or at most two if you need a backup) which you keep to yourself somewhere safe and secure. After someone encrypts a message with a copy of your public PGP key and you receive it, Thunderbird/Enigmail will use your private key to decrypt it, once you enter a password that you set when you first generate the pair of keys.

**Tom Sanderson (TCIJ)**

### Second computer and phone

If you are in Risk Level Four, it is possible that you are a target of government or private intelligence operations and they will seek to get programs or equipment into your computer that will inform them of what you are up to. This might include location devices or keystroke transmitters. The latter will help get to know your passwords.

### Endpoint

As InfoSec people will tell you, all the encryption and security systems are negated if your endpoint is compromised. For those engaged against state actors you may be subject to attack by a system like Pegasus. They send highly tailored Trojan messages to install their software. Pegasus is capable of reading text messages, tracking calls, collecting passwords, tracing the location of the phone, and gathering information from apps. The company that created the spyware, NSO Group stated that they provide 'authorized governments with technology that helps them combat terror and crime'. It is believed that human rights activists and journalists have been targeted by government security organisations using this system.

*all the encryption and security systems are negated if your endpoint is compromised.*

# Part II – A Changing Legal Situation: *From Demonstrating Truth to Public Interest*

# Key Laws Deployed Against Journalists

*These acts are meant to balance competing interests, namely those of the sources seeking anonymity, a journalist seeking to protect the source, and the legitimate interests of the state in seeking information for the purposes of policing, and administrating justice.*

In November 2018 the UK Financial Conduct Authority (FCA) seized six-years' worth of call records from the telecomm provider to a *Daily Mail* financial journalist and exposed his sources. This was done at the request of FCA's French counterparts. Details of calls by journalist Geoff Foster from 4 July 2007 to 14 June 2013, including the telephone numbers and identities of his sources, were handed over to the Autorité des Marchés Financiers (AMF, Financial Markets Authority). Foster has been fined -40,000 by the AMF for alleged insider trading, relating to two 'market report' articles published in 2011 and 2012 in which he reported on a possible bid from French luxury goods conglomerate Louis Vuitton Moët Hennessy to buy rival fashion retailer Hermès. It is alleged that he improperly revealed 'privileged information' in advance of publication, leading to the insider trading charge. A spokesperson for Foster and *Daily Mail* publisher Associated Newspapers has branded the court decision 'deeply troubling' and as having 'serious implications for financial journalism'. The FCA is likely to have used the Regulation of Investigatory Powers Act 2000, to obtain the data.

Where the state is seeking information, key laws deployed against journalists include the Police and Criminal Evidence Act 1984 (ss. 9, 11, 13, 14 and sch. 1), the Terrorism Act 2000 (s. 37 and sch. 5, para 5 and 6), the Criminal Justice Act 1987 (s. 2), the Inquiries Act 2005 (s. 21) and the Financial Services and Markets Act 2000 (s. 13). This is not a comprehensive list, however.

Each of the above laws sets out the circumstances in, and the purposes for, which a state authority can obtain information. These acts are meant to balance competing interests, namely those of the sources seeking anonymity, a journalist seeking to protect the source, and the legitimate interests of the state in seeking information for the purposes of policing, and administrating justice.

For example, the Police and Criminal Evidence Act 1984 includes rules for accessing journalistic material, i.e. content. It differentiates journalistic material from other information and classifies it as 'special procedure material' or 'excluded material' depending on whether it is held under a duty of confidence (Townend and Danbury 2017). Schedule 1 provides access criteria for 'special procedure material'. Excluded material cannot normally be accessed under the Police and Criminal Evidence Act 1984 (para. 3 of sch. 1 comprises a savings clause for earlier legislation under which excluded material could be obtained, for example the Official Secrets Act 1920). Such journalistic material may also be acquired via terrorism-related legislation such as the Terrorism Act 2000.

*…even these qualified protections have been undermined in recent times, and concerns about the ability to protect journalistic sources from the state are becoming more acute. This is because these delicate balances risk being outdated by contemporary technological and legal developments*

Both the Police and Criminal Evidence Act 1984 and the Terrorism Act 2000 contain 'access conditions' including whether the material would be in the public interest to disclose, but judicial discretion is also relevant and the European Convention on Human Rights (ECHR) Article 10 can be taken into account. The Police and Criminal Evidence Act 1984 focuses on protecting content: there is no absolute protection for sources under UK law. Nevertheless, the protection under the Act for excluded (i.e. confidential) source material is reasonably strong, and, while the Act's safeguards for 'special procedure' material are weaker, they were said to work. The protections from disclosure where the Terrorism Act 2000 bites, however, are weaker still.

What is important, however, is that even these qualified protections have been undermined in recent times, and concerns about the ability to protect journalistic sources from the state are becoming more acute. This is because these delicate balances risk being outdated by contemporary technological and legal developments. In practice, the rulings of the ECtHR combined with domestic law, provide a list of substantive and procedural factors that need to be taken into account by a court, when deciding whether to permit disclosure of a journalists' source (Townend and Danbury 2017).

**The substantive factors include:**

- The extent of the proposed interference with freedom of speech;
- General and particular public interests at stake in dissemination of the sources' information to the public;
- Objectives said to justify disclosure;
- The motive and conduct of source;
- The journalist's conduct;
- Whether confidentiality was expressly promised to the source;
- Other rights of the journalists, sources and third parties (Danbury and Townend 2017).

**The Regulation of Investigatory Powers Act 2000** has been extensively used for seizing journalists' data and records. It can completely prevent a journalist from working for long periods. There was an overhaul of the legislation in 2016 and before *Press Gazette*'s Save Our Sources campaign, which in 2015 succeeded in making any such requests for journalistic material subject to judicial sign off. (This is not a comprehensive list.)

The sole proper procedure for acquiring unpublished journalistic material is an application for a Production Order under s. 9 (1) and Schedule 1 of the Police and Criminal Evidence Act 1984. However there are other legal routes by which the state can try and obtain journalists' work product or source material.

1. Using Norwich Pharmacal Route – used in interbrew and also Goodwin, for example (see 2TG Commercial Fraud Team 2018, Sjøvoll, 2017).
2. Application for a witness summons under s.2 of the Criminal Procedure (Attendance of Witnesses) Act 1965. This is being increasingly (and controversially) deployed by police close to trial in part because of their nervousness around their third party disclosure obligations. Under the Attorney General's guidelines, the Crown Prosecution Service (CPS) may be under an obligation to seek third-party material. Case law states a witness summons cannot be used for the purposes of obtaining disclosure material, or material solely for the purposes of cross-examination. (See the House of Lords in R (B) v Derby Magistrates [1996] AC 487; and the Court of Appeal (Criminal Division) in R v Basra (Wasted Costs) [1998] PNLR 535.)

The Investigatory Powers Act (2016) is the legislation under which sources are most likely to be disclosed. Crucially under the Investigatory Powers Act, the media organisation and journalist does not have notice of the application (unlike the Police and Criminal Evidence Act 1984) so you don't know whether the authorities are seeking to find your source.

Oversight for these operations will come with a new 'double-lock', where any intercept warrants will need ministerial authorisation before being adjudicated by a panel of judges, who will be given power of veto. This panel will be overseen by a single senior judge, the newly created Investigatory Powers Commissioner.

Also, you do not go before a court for the issues to be determined. When reviewing a person's decision to issue a warrant for the decryption of communications or communications data, the Investigatory Powers Commissioner needs to determine that:

1. The warrant is necessary on the grounds provided for in the Investigatory Powers Act, for example, national security; and
2. The behaviour allowed for, under which the warrant has been issued, is proportionate to the desired outcome of that behaviour.

The only exception to this decision-making process is in the most urgent of circumstances, although the warrant must subsequently receive approval from the Investigatory Powers Commissioner (s.24 of the Investigatory Powers Act 2016).

The General Data Protection Regulations (GDPR) forms part of the data protection regime in the UK, together with the new Data Protection Act 2018. The main provisions of this apply, like the GDPR, from 25 May 2018. Many journalists should register as data controllers. Under the GDPR, you will pay an annual fee, depending on your size or turnover, but this will now be £40, £60 or £2900. VAT is nil in all cases. You should use the ICO assessment tool (**ico.org.uk/fee-self-assessment**) to confirm how much you need to pay.

# Box 7 Further guidance on GDPR

Guide to the General Data Protection Regulation (GDPR)
**https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/**

The ICO guide for the media on GDPR
**https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf**

NUJ information on GDPR
**https://www.nuj.org.uk/news/dm18-gdpr/**

'Personal data' is any information that relates to a living individual who can be identified from that information, or from that and other information in our possession or likely to come into our possession. Personal data can include email addresses or telephone numbers.

An exemption can apply if you process personal data for journalistic purposes.
The exemption relieves you from your obligations regarding the GDPR's provisions on:

- All the principles, except the security and accountability principles;
- The lawful bases;
- The conditions for consent;
- Children's consent;
- The conditions for processing special categories of personal data and data about criminal convictions and offences;
- Processing not requiring identification;
- The right to be informed;
- All the other individual rights, except rights related to automated individual decision-making including profiling;
- The communication of personal data breaches to individuals;
- Consultation with the ICO for high risk processing;
- International transfers of personal data; and co-operation and consistency between supervisory authorities.

However, the exemption only applies to the extent that:

- As controller for the processing of personal data, you reasonably believe that compliance with these provisions would be incompatible with the special purposes (this must be more than just an inconvenience);
- The processing is being carried out with a view to the publication of some journalistic material;
- And you reasonably believe that the publication of the material would be in the public interest, taking into account the special importance of the general public interest in freedom of expression, any specific public interest in the particular subject, and the potential to harm individuals.

Note: if data is lost there is now a duty to report that to the Information Commissioners Office.

# A Change of Direction in Media Law

*…changes to media law have resulted in a move away from the need to evidence the truth of your story to being able to demonstrate you had a public interest justification to investigate at all.*

Senior editors and media lawyers suggest that changes to media law have resulted in a move away from the need to evidence the truth of your story to being able to demonstrate you had a public interest justification to investigate at all. The best means of demonstrating the truth was to retain all the evidence you collected. However, now that an action under libel or defamation has to be launched with a year, if it has not been, then there is no need to retain the evidence. The focus has moved to public interest and you need to be able to demonstrate that your acquisition of information and its retention has a strong demonstrable public interest defence. Lawyers will use the burgeoning data laws to challenge your activities. You are likely to be challenged about the data you collected and whether it was justified from an early stage in your investigation.

In the UK there is no privacy law passed in Parliament. However, senior editors and media lawyers say that, in effect, privacy law has emerged by stealth. There are several areas of law which together amount to a privacy law, including confidentiality law, data protection law and misuse of private information law.

The Editor of the *Financial Times*, Lionel Barber, noted at the James Cameron Lecture 2018 that over the past 15 years or so, this area of law has developed apace. He observes that initially, the courts stretched the equitable principles of 'breach of confidence' to create something akin to a privacy right. He notes that from the time the supermodel Naomi Campbell ultimately won her case against *Mirror Group Newspapers* in the House of Lords after she was photographed coming out of a Narcotics Anonymous meeting:

> *Subsequently and almost seamlessly, we have witnessed a new privacy tort of 'misuse of private information' (or MPI, as lawyers refer to it). Editors have become used to having to weigh up competing interests of freedom of expression versus any reasonable expectation of privacy — as per articles 10 and 8 respectively of the European Convention on Human Rights. Now, the latter is not an absolute right, and it would not be so troublesome were it not for the mushrooming of data protection law, which has added to the privacy hazards facing the press.*
>
> *What concerns me most is the way it is being used to cover digital/online journalism, specifically via 'personal data'. Complainants are increasingly resorting to data protection law to attack or fetter journalism, with so-called subject access requests and rectification or deletion requests.*

*Lawyers will use the burgeoning data laws to challenge your activities*

## A Change of Direction in Media Law (Continued)

In 2017, the NUJ lobbied politicians about data protection and the impact on public interest journalism. At the time, the Union said:

> *The NUJ is concerned that new data protection laws will be used against media organisations and freelance journalists to force them to amend or delete information, or surrender personal data gathered in the course of their work. The media have previously had exemptions in law known as 'special purposes' — and if public interest tests are satisfied. The NUJ is concerned that the provisions may no longer offer adequate protection as legal claims test data privacy rules in court. The union is keen to ensure the law is not used against investigative journalism in instances where large amounts of leaked data are held by a media organisation.*

Pia Sarma, editorial legal director at *The Times* and *Sunday Times*, has said: 'We are getting told when we go to subjects for comment that we can't process their personal data, which raises the concern that post-publication we might be mired in a costly action.' (Thompson 2017) For instance, some subjects named in the *Sunday Times*' 2015 investigation into blood doping in athletics (which involved the records of 12,359 blood tests taken from more than 5,000 athletes) tried to use data protection laws to prevent their personal information being released. According to Sarma, data complaints were now being added 'to almost every threat we get' (Thompson 2017). *The Guardian News & Media* have also said: 'While it is absolutely right that we respect the personal data of citizens, we have seen an increasing trend for powerful complainants to use data protection law as a way to stymie public interest investigations into their activities.' The *Financial Times* has also received several complaints citing data protection laws (Thompson 2017).

A libel claim can be brought only if there has been 'serious harm' to someone's reputation, and it must be issued within a year of the report first being published. With data legislation there is no such time limit and it is not necessary to prove any reputational or financial impact, only 'distress'. Data protection laws should protect consumers from intrusive marketing and other commercial practices. They should not provide a backdoor route to a claim if a libel or privacy action looked likely to fail. Yet, the *Financial Times* has reported that in a recent legal case, Prince Moulay Hicham of Morocco sued Elaph, an Arab news website registered in the UK, for libel. In addition, the prince's lawyers added a claim under the Data Protection Act 1998 that Elaph had published inaccurate personal data. In November 2016 the Court of Appeal ruled that the Data Protection Act 1998 claim could form 'an appropriate alternative means of redress' if Elaph's article was not deemed defamatory (White & Case LLP 2017).

Individuals can make a written request to find out what information a data controller holds about them, where it was obtained from, and ask for copies of the information. The data controller must consider whether information (or some of it) can be provided without undermining its journalistic activities. The journalism exemption can be applied to refuse the request if providing the information would be incompatible with journalism (see Box 8). Information about other people only needs to be supplied if that individual consents or it is reasonable to supply it without that consent.

# **Box 8** Subject access requests

**Under data protection laws:**

- Individuals have the right to access their personal data.
- This is commonly referred to as 'subject access'.
- Individuals can make a subject access request verbally or in writing.
- You have one month to respond to a request.
- You cannot charge a fee to deal with a request in most circumstances.

**Individuals have the right to obtain the following from you:**

- Confirmation that you are processing their personal data;
- A copy of their personal data; and
- Other supplementary information – this largely corresponds to the information that you should provide in a privacy notice.

An individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone). Therefore, it is important that you establish whether the information requested falls within the definition of personal data. For further information about the definition of personal data please see guidance on what is personal data.

**In addition to a copy of their personal data, data controllers also have to provide individuals with the information that includes:**

- The purposes of your processing;
- The categories of personal data concerned;
- The recipients or categories of recipient you disclose the personal data to;
- Your retention period for storing the personal data or, where this is not possible, your criteria for determining how long you will store it;
- The existence of their right to request rectification, erasure or restriction or to object to such processing;
- The right to lodge a complaint with the ICO or another supervisory authority;
- Information about the source of the data, where it was not obtained directly from the individual;

See ICO guidelines for full list:
**https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf**

## Scotland

The law in Scotland is different in some aspects to England and Wales, whereas other laws are the same. After reports that Police Scotland has been tracking journalists and their sources, the Scottish Newspaper Society first requested details about the use of the Regulation of Investigatory Powers Act 2000 to track journalists and their sources in October 2014. For fourteen months the force stuck rigidly to a refusal to confirm or deny that any information existed. The Scottish Newspaper Society appealed to the Scottish Information Commissioner and the force finally admitted to tracking journalists' sources on 12 occasions in the previous four years. Throughout this period both the Sunday Herald and the Sunday Mail had kept up the pressure, particularly in the knowledge that the Sunday Mail's story about the investigation into the murder of Emma Caldwell was central to a snooping operation, in contravention of the then new guidelines. The Scottish Newspaper Society took the view that Police Scotland was suggesting that journalists have no right to defend the principle of protecting sources, or that the press should have no role in the system of checks and balances on the powerful (The Scottish Newspaper Society 2015).

# The Constant Erosion of Press Freedom

When it comes to suspicion of terrorism issues, the agencies can fish through journalists' communications and/or equipment using investigatory powers that mostly do not need a judge to sign off; they just need to be signed off internally by one of the agencies with the powers to use them, such as the Home Office, police and others. There is a tendency by law enforcement to frame their inquiries as investigating terrorism: that opens a wider range of powers to them and is harder for judges to resist when asked to sign warrants.

Further evidence of the dangers of covering terrorism and intelligence stories for journalists, even if they are historical, came in late August 2018. The boldness of the police in acting against two Northern Ireland journalists shows how much the political climate has changed. Some 100 police officers raided the Belfast homes and an office of journalists Trevor Birney and Barry McCaffrey, both of whom had worked with the Oscar-winning documentary filmmaker Alex Gibney on the 'No Stone Unturned' documentary about a June 18 1994 massacre at a pub in Loughinisland in Northern Ireland. Two men, their identities hidden beneath balaclavas, had opened fire, killing six patrons (all Catholics who were shot in the back). The local members of the paramilitary loyalist group, the Ulster Volunteer Force, were immediately suspected. However, until Gibney's film, and based on the investigations of producer Birney and former *Irish News* reporter McCaffrey, the terrorists, including the primary gunman, had not been named. Birney was arrested in the early morning in front of his wife and children after a judge had signed the search warrants. The judge signed the warrants ex parte under an unprecedented approach somewhere between the provisions in the Police and Criminal Evidence Act 1984 and a production order. The police told the judge that they were investigating the theft of documents, handlings stolen documents, data protection breaches and breaches of the Official Secrets Act.

There is an ongoing judicial review to challenge the ability of the police to access all the documents seized during the arrests, especially the information that is not related to the documentary. The police removed all computing equipment from the two mens' home (including his eight-year-old daughter's broken, pink mobile phone) and removed material from the production office including material that related to other projects that the production team were working on. Supported by the NUJ, the two journalists had not been charged at the time of writing but questioned about being in possession of stolen documents, and will be on bail until March 2019. The police said the arrests had been triggered by a complaint from the Police Ombudsman of Northern Ireland. In an interview with the *Irish Times*, the Police Ombudsman of Northern Ireland said that he did not make a complaint but briefed the Police Service of Northern Ireland that the journalists had access to the confidential document (which identifies by name the suspected assailants). Given that the suspects are still free, arresting journalists over stolen documents feels very much like a return to the bad days of the 1970s.

Alex Gibney told the Hollywood Reporter:

> *I think their purpose was to send a message, and the message is 'Don't engage in these kind of enquiries into past police behavior.' I think this was an act of intimidation. They were concerned, as all governments are, when journalists obtain classified material. Nevertheless, there's kind of an assumption, particularly under US law but also under UK law, that journalists are operating in the public interest, and if there are leaks, the government may go after people in the government who may have leaked that material, but not the journalists who publish it.*

He noted that the film intended to hold the UK government to account for collusion between paramilitary gangs, the police and the army: that is to say, for an active role in aiding and abetting criminal behavior about a massacre that happened in 1994.

What this means is that journalists working on controversial cases increasingly face having their working materials and equipment seized. That is a stark reminder of the importance of keeping your data secure.

For further resources and learning material: go to InfoSec Bytes – a series of videos produced by CIJ that explain everything from simple to advanced info-security for journalists. See: **https://www.youtube.com/channel/UCfET6btFpe1e0CRGTFOulNg**

# References:


2TG Commercial Fraud Team (2018) *A Practical Guide To: Norwich Pharmacal Orders*. Available at: **http://www.2tg.co.uk/wp-content/uploads/2018/05/2TG-Practical-Guide-to-Norwich-Pharmacal-Orders-Summer-2018-1.pdf**
Bakir V (2018) *Intelligence Elites and Public* Accountability. Abingdon: Routledge.

Bakir V (2015) Veillant Panoptic Assemblage: Critically Interrogating Mutual Watching through a Case Study of the Snowden Leaks. ***Media and Communication*** 3(3). DOI: **http://dx.doi.org/10.17645/mac.v3i3.277**

Carlo S and Kamphuis A (2014) *Information Security for Journalists*. London: the Centre for Investigative Journalism.

Contempt of Court Act 1981. Available at: **https://www.legislation.gov.uk/ukpga/1981/49/section/10**

Council of Europe, Human Rights Europe (2018) Court: Some Aspects of UK Surveillance Regimes Violate Conventions. Available at: **http://www.humanrightseurope.org/2018/09/court-some-aspects-of-uk-surveillance-regimes-violate-convention/**

Cox J (2016) Watchdog Finds UK Cops Snooped on Journalists' Sources Without Approval. *Motherboard*, [online] 8 September. Available at: **https://motherboard.vice.com/en_us/article/z43wye/watchdog-iocco-finds-uk-cops-snooped-on-journalists-sources-without-approval**

Goodwin B (2018a) Top 10 stories on national security in 2018, *Computer Weekly*, [online]. 28 December. Available at: **https://www.computerweekly.com/news/252454532/Top-10-stories-on-National-Security-in-2018**

Goodwin B (2018b) UK faces 10 cyber attacks a week as hostile states step up hacking, says NCSC. *Computer Weekly*, [online] 16 October. Available at: **https://www.computerweekly.com/news/252450677/UK-faces-10-cyber-attacks-a-week-as-hostile-states-step-up-hacking**

Griffin A (2016) Everyone who can now see your entire internet history, including the taxman, DWP and Food Standards Agency. *The Independent*, [online] 24 November. Available at: **https://www.independent.co.uk/life-style/gadgets-and-tech/news/investigatory-powers-bill-act-snoopers-charter-browsing-history-what-does-it-mean-a7436251.html**

Investigatory Powers Act 2016. Available at: **http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted**

Lashmar P (2017) No more sources? The impact of Snowden's revelations on journalists and their confidential sources. *Journalism Practice*. 11(6): 665-688. **https://doi.org/10.1080/17512786.2016.1179587**

Lashmar P (2018) Journalistic Freedom and Surveillance of Journalists post-Snowden. In Franklin B and Eldridge SA. *The Routledge Handbook of Developments in Digital Journalism Studies*. Routledge.

Mann S and Ferenbok (2013). New media and the power politics of sousveillance in a surveillance-dominated world. *Surveillance & Society*, 11(1/2), 18-34. DOI **https://doi.org/10.24908/ss.v11i1/2.4456**

Marthews A and Tucker CE (2017) Government surveillance and internet search behaviour. *SSRN*. **http://dx.doi.org/10.2139/ssrn.2412564**

McStay A (2017) *Privacy and the Media*. Sage.

Media Lawyer Staff (2017) Chief constable apologises to journalists over phone snooping. *HoldtheFrontPage*, [online] 5 January. Available at: **https://www.holdthefrontpage.co.uk/2017/news/chief-constable-apologises-to-journalists-over-phone-snooping/**

O'Carroll L (2015) Met police broke law by accessing Sun reporter's phone records over Plebgate. *The Guardian*, [online] 17 December. Available at: **https://www.theguardian.com/media/2015/dec/17/met-police-broke-law-by-accessing-sun-reporters-phone-records-over-plebgate**

PEN (2013) *Chilling effects: NSA Surveillance drives U.S. writers to self-censor*. [pdf] New York: PEN American Center. Available at: **http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf**

Penney JW (2016) Chilling Effects: Online Surveillance and Wikipedia Use, *Berkeley Technology Law Journal* 31(1). **https://doi.org/10.15779/Z38SS13**

Pew Research Center (2015) *Investigative journalists and digital security: perceptions of vulnerability and changes in behaviour*. [pdf] Available at: **http://www.journalism.org/2015/02/05/investigative-journalists-and-digital-security/**

Police and Criminal Evidence Act (PACE) 1984. Available at: **http://www.legislation.gov.uk/ukpga/1984/60/contents**

## References (Continued)


Ponsford D (2016) Surveillance court awards zero compensation to Sun reporter after police illegally viewed his call records. *Press Gazette*, [online] 4 February. Available at: **https://www.pressgazette.co.uk/surveillance-court-awards-zero-compensation-sun-reporter-after-police-illegally-viewed-his-call/3/**

Press Gazette (2016) Local reporter Sally Murrer: 'Police surveillance destroyed my life, the snooper's charter absolutely terrifies me'. *Press Gazette*, [online] 29 July. Available at: **https://www.pressgazette.co.uk/local-press-reporter-police-surveillance-destroyed-my-life-the-snoopers-charter-absolutely-terrifies-me/**

Privacy International (2018) *Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards*. April. **https://privacyinternational.org/sites/default/files/2018-04/Secret%20Global%20Surveillance%20Networks%20report%20web%20%28200%29.pdf**

Regulation of Investigatory Powers Act (RIPA) 2000. Available at: **https://www.legislation.gov.uk/ukpga/2000/23/contents**

Rozenberg J and Halliday J (2015) Police will need judge's permission to access journalists' phone and email records. *The Guardian* [online] 4 February. Available at: **https://www.theguardian.com/world/2015/feb/04/police-600-applications-trace-journalist-sources-snopping-watchdog**

Seitz J (2019) How To Blow Your Online Cover With URL Previews. *Bellingcat*, [online] 4 January. Available at: **https://www.bellingcat.com/resources/how-tos/2019/01/04/how-to-blow-your-online-cover-with-url-previews/**

Serious Organised Crime & Police Act 2005. Available at: **https://www.legislation.gov.uk/ukpga/2005/15/contents**

Stoycheff E (2016) Under surveillance: examining Facebook's spiral of silence effects in the wake of NSA internet monitoring. *Journalism & Mass Communication Quarterly*, 93(2), pp.1–16. **https://doi.org/10.1177/1077699016630255**

Sjøvoll K (2017) Online Publication Claims: Norwich Pharmacal orders and Jurisdiction Issues. *Informs Blog*, [online]. Available at: **https://inforrm.org/2017/10/26/online-publication-claims-norwich-pharmacal-orders-and-jurisdiction-issues-kirsten-sjovoll/**

Terrorism Act 2000. Available at: **https://www.legislation.gov.uk/ukpga/2000/11/contents**

The Anti-Terrorism Crime & Security Act 2001. Available at: **https://www.legislation.gov.uk/ukpga/2001/24/contents**

The Scottish Newspaper Society (2015) *Snooping on journalists' sources: the hole Police Scotland can't stop digging*. [online] 18 December. Available at: **http://www.scotns.org.uk/snooping-on-journalists-sources-the-hole-police-scotland-cant-stop-digging/**

The Washington Post (2018a) Shocked by Trump aggression against reporters and sources? The blueprint was drawn by Obama. *The Washington Post,* [online] 8 June. Available at: **https://www.washingtonpost.com/lifestyle/style/shocked-by-the-trump-aggression-against-reporters-and-sources-the-blueprint-was-made-by-obama/2018/06/08/c0b84d88-6b06-11e8-9e38-24e693b38637_story.html?utm_term=.4dce7ace2361**

The Washington Post (2018b) Hands off my data! 15 default privacy settings you should change right now. *The Washington Post*, [online] 1 June. Available at: **https://www.washingtonpost.com/news/the-switch/wp/2018/06/01/hands-off-my-data-15-default-privacy-settings-you-should-change-right-now/?utm_term=.11848a839c0d**

Thompson B (2017) UK Media warn data rules used to stifle journalism. *Financial Times*, [online] 17 October. Available at: **https://www.ft.com/content/d3d1e6a4-9d34-11e7-9a86-4d5a475ba4c5**

Tobbit C (2018) 'Extremely good day for journalism' as ECHR rules UK Government surveillance regime violated freedom of the press. *Press Gazette*, [online] 13 September. Available at: **https://www.pressgazette.co.uk/extremely-good-day-for-journalism-as-echr-rules-uk-government-surveillance-regime-violated-freedom-of-the-press/**

Townend J and Danbury R (2017) *Protecting Sources and Whistleblowers in a Digital Age. Information Law and Policy Centre, Institute of Advanced Legal Studies, supported by Guardian News and Media*. [online] Available at: **https://infolawcentre.blogs.sas.ac.uk/files/2017/02/Sources-Report_webversion_22_2_17.pdf**

White & Case LLP (2017) *Defamation and data protection claims can be brought in parallel*, 15 March. Available at: **https://www.jdsupra.com/legalnews/defamation-and-data-protection-claims-79569/**

Williams N, McMenemy, D and Smith, L (2018) *Scottish Chilling: Impact of Government and Corporate Surveillance on Writers*. Scottish Pen and University of Strathclyde. Available at: **https://strathprints.strath.ac.uk/66291/8/Williams_etal_PEN_2018_Scottish_chilling_impact_of_government_and_corporate_surveillance_on_writers.pdf**