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

[redacted]

Abridged Version

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. If so, use burner phones, and if need be, multiple burner phones. 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 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).