The Perugia Principles for Journalists Working with Whistleblowers in the Digital Age

blueprint for FREE SPEECH

The Origin of the Perugia Principles

The Perugia Principles were developed by the authors in partnership with a roundtable of 20 international journalists and experts hosted by Blueprint for Free Speech in Perugia, Italy in April 2018. The authors then consulted with the broader investigative journalism, legal and academic communities to refine the Principles.

To contact us: info@blueprintforfreespeech.net
or via our web contact form at: www.blueprintforfreespeech.net

Authors

Julie Posetti
Senior Research Fellow, Reuters Institute for the Study of Journalism at the University of Oxford

Dr Suelette Dreyfus
Academic Specialist, University of Melbourne. Executive Director, Blueprint for Free Speech

Naomi Colvin
Program Director UK, Blueprint for Free Speech

Design: Garreth Hanley

Acknowledgements

The authors gratefully acknowledge the support of the following people and organisations in producing this handbook:

The Open Society Initiative for Europe within the Open Society Foundations, The Reuters Institute for the Study of Journalism at the University of Oxford, The Thomson Reuters Foundation, The University of Melbourne, Nishith Desai Associates and S. Welsh.

Foundation Partner Organisations

Reuters Institute for the Study of Journalism (RISJ) at the University of Oxford

International Center for Journalists (ICFJ)

Global Investigative Journalism Network (GIJN)

World Editors Forum

Signals Network

blueprint for FREE SPEECH

The Perugia Principles for Journalists

Working with Whistleblowers in the Digital Age

By Julie Posetti, Dr Suelette Dreyfus and Naomi Colvin

Table of Contents

blueprint for FREE SPEECH

"We're being forced to act like spies, having to learn trade craft and encryption and all the new ways to protect sources. But we are not an intelligence agency. We're not really spies. So, there's going to be a time when you might make a mistake or do something that might not perfectly protect a source. This is really hard work. It's really dangerous for everybody."

James Risen, Senior National Security Correspondent at The Intercept and director of First Look Media's Press Freedom Defense Fund [1]

12 PRINCIPLES FOR WORKING WITH WHISTLEBLOWERS IN THE DIGITAL AGE

1. First, protect your sources. Defend anonymity when it is requested
2. Provide safe ways for sources to make 'first contact' with you, where possible
3. Recognise the costs of whistleblowing for the whistleblower, and prompt them to think through ahead of time how to cope when the story breaks
4. Verify material focusing on the public interest value of the information, not on your view of the attitudes or opinions of the source or whistleblower
5. Take responsibility for your digital defence and use encryption. Even though encryption may not completely defend your source, it offers important first-line protection.
6. Determine the biggest threats to you and your source, and what specific steps you need to take to protect both of you
7. Explain the risks of digital exposure to your source or whistleblower. On sensitive stories, train your whistleblowers in basic digital security
8. Publish original documents and datasets in their entirety where possible *and* safe to do so, recognising the importance of datasets in stories
9. Securely delete data provided by sources, when asked, to protect confidential sources, consistent with ethical, legal and employer obligations
10. Ensure any digital drop boxes for confidential sources and whistleblowers offer a good level of security, and, for higher-risk materials, anonymity
11. Understand the country, regional and international legal and regulatory frameworks for protecting confidential sources and whistleblowers
12. Encourage news publishers to practice their responsibility to provide proper data security for journalists, sources and stored materials, along with appropriate training and policies to guide journalists

Source Protection in the Digital Age

Without confidential sources and whistleblowers, many acts of investigative storytelling - from Watergate to the Snowden Files and the Panama Papers – might never have surfaced. Such sources may require anonymity to protect them from physical, economic or professional reprisals in response to their revelations, published in the public interest.

This is why there is a globally established ethical obligation upon journalists[2] to avoid revealing the identity of their confidential sources. There is also a strong tradition of legal source protection internationally, in recognition of the vital function that confidential sources play in facilitating 'watchdog' or 'accountability' journalism. In some cases, it is also a legal right, or even a legal requirement. For example, in Sweden the law protecting sources is so strict that journalists can be prosecuted and jailed for revealing their confidential sources' identities without their permission[3]. Where the legal line is drawn, and how it is interpreted, varies around the world but the principle that sets confidentiality as the norm, and disclosure as the exception, is the generally-accepted standard.[4]

In many countries, however, such laws are non-existent, or routinely flouted. And while these laws, where they do exist, might help shield journalists from being compelled to reveal their confidential sources, they do not protect the confidential sources themselves from exposure or prosecution, including the whistleblowers among them. This is one reason why the UN-published study Protecting Journalism Sources in the Digital Age[5] recommended that:

> **To optimise benefits, source protection laws should be strengthened in tandem with legal protections extended to whistleblowers, who constitute a significant set of confidential journalistic sources**

But there is a host of new Digital Age threats challenging legal and ethical frameworks designed to support investigative journalism based on information provided by confidential sources and whistleblowers. These global threats have been described as "eroding", "compromising" and "undercutting" existing protections[6]. They include:

- The limitations of analogue era source protection/shield laws in dealing with digital information (e.g. where reporter's paper notebooks are protected but hard drives, smart phones and metadata are not).
- Interception of confidential communications by State, corporate or criminal actors.
- Undercutting of legal protections for source confidentiality via mass and targeted surveillance. For example: confidential journalistic communications are frequently caught in the 'nets' of mass surveillance.
- The overreach of national security and anti-terrorism justifications for breaching legal protections and covertly accessing journalistic communications (e.g. metadata).
- Government requirements that third-party intermediaries i.e. social media companies, phone companies, Internet Service Providers (ISPs) retain metadata for lengthy periods and hand it over to authorities on demand - with or without warrants.
- Self-exposure by confidential sources and whistleblowers using insecure digital methods as a first point of contact with journalists.
- Low levels of risk awareness and digital defence training among journalists and within news organisations.
- Moves by States to criminalise or override encryption.
- The proliferation of leak investigations targeting journalists in source-fishing exercises (including by law enforcement agencies).
- The deliberate targeting of journalists and their sources in online disinformation campaigns designed to chill information flows.[7]

These risks are exacerbated by digital era methods of journalistic communication and reporting (e.g. email, smartphones, messaging apps, social media activity) and the 'internet of things' - from smart watches and fitness tracking apps to internet-enabled glasses that map our movements, our likes and dislikes, our connections and our conversations.

It's not all bad news, is it?

The Digital Age has also brought many opportunities for high impact investigative journalism – as evidenced by the Snowden Files and the Panama Papers. It is now possible for whistleblowers to move and leak masses of valuable data in the public interest on an unprecedented scale, with appropriately strong digital security methods in place. In fact, it is because of these possibilities that the International Consortium for Investigative Journalists' Gerard Ryle has labelled the Digital Era as a "Golden Age for investigative journalism."[8] However, this is also the era in which whistleblowers are being jailed because security agencies have unprecedented powers of interception and discovery. It is not an equal struggle when your adversary is a national security agency. In the case of US whistleblower Reality Winner, her identity appears to have been discovered via analysis of the embedded metadata from a printed document provided by The Intercept's journalist to the NSA for verification and comment.[9]

So, is it even possible to guarantee you will keep your source's identity confidential in the Digital Age? And is it ethical to promise source confidentiality if you recognise the increased risks of exposure? At the very least, should you acknowledge these threats to confidential sources and whistleblowers and add caveats to your commitments? And what other obligations might you or your news organisation have to your source if they are exposed and placed at risk? In the Reality Winner case, The Intercept provided legal support and contributed financially to a grass roots campaign to defend her.[10]

So, what are journalists' ethical obligations to confidential sources and whistleblowers in the Digital Age?

> **"Investigative reporting is not a science...there's no playbook for exactly how to deal with sources. It's a very human process." James Risen**

Even in the Surveillance State, the 'human' aspects of the relationship between journalists, confidential sources and whistleblowers remain paramount. Such relationships have always involved risk, tension, stress, negotiation, and a precarious dance of trust. And they have always been unequal relationships: it is inevitably the whistleblower or confidential source who is taking the greatest risk in seeking to facilitate the revelation of public interest information that powerful people, governments, criminals and companies would like to remain hidden. The nature of this relationship therefore historically entailed significant ethical challenges and obligations. But in the Digital Age a host of new threats exist, as outlined above. That is why this handbook recommends the re-evaluation of ethical obligations regarding source protection. Responses to this challenge could include:

- Adapting research and reporting practices to address Digital Age risks.
- Embracing encryption as a minimum, though not foolproof, standard operating procedure.
- Upgrading digital safety, privacy enhancing tools, and security skills in light of these new threats.
- Raising awareness of digital communications risks with confidential sources and whistleblowers.
- Assisting confidential sources and whistleblowers with training, resources and tools (e.g. secure digital drop boxes and encrypted messaging apps like Signal[11] to enable secure digital communications with reporters).
- Recognising the risks of metadata and 'digital detritus'.[12]

Are confidential sources and whistleblowers the same thing?

It is important to note that confidential sources and whistleblowers are not interchangeable terms. Whistleblowers are a subset of confidential journalistic sources but not all whistleblowers seek to involve the news media in their attempts to reveal information in the public interest (i.e. many rely on internal reporting mechanisms within companies and government institutions). So, not all confidential sources are whistleblowers, and not all whistleblowers require confidentiality. This handbook focuses on journalists' dealings with whistleblowers. However, while differentiating between confidential sources and whistleblowers is important, in general the broad principles of source protection apply to both categories of sources.

Developing Digital Age Guidelines for Doing Journalism with Whistleblowers

The 12 principles outlined in this handbook were developed in consultation with Blueprint for Free Speech, the Reuters Institute for the Study of Journalism (RISJ) at the University of Oxford, the International Center for Journalists (ICFJ), the World Editors Forum within The World Association of Newspaper and News Publishers (WAN-IFRA) and The Signals Network. They were informed by a process of academic research that involved interviews and focused discussions with 20 international investigative journalists and associated experts working in Western Europe, Eastern Europe, the UK, the Middle East, Africa, the US and Asia.[13] These interviews and focused discussions were supplemented by contributions from legal experts,[14] whistleblowers and whistleblower-advocates. The 'Perugia Principles' take their name from the main research site for this research: Perugia, Italy, home of the annual International Journalism Festival (IJF). During the 2018 edition of the conference, lead author Julie Posetti convened and facilitated a 'round table' discussion involving international experts in the field, to test and focus the original 20 draft principles developed during the first phase of research (which included an online survey).[15]

Putting the Principles into Practice

Principle 1: First, protect your sources. Defend anonymity when it is requested

"I just thought I was doing what journalists are supposed to do, which is protect your sources - if the government tries to force you to tell who your sources are, you refuse."
James Risen

Putting this into practice

- Treat the confidential source or whistleblower with dignity and respect. Avoid characterising the relationship as purely transactional.
- It is generally accepted that a journalist's commitment to protect the anonymity of confidential sources and whistleblowers should only be breached in the most exceptional circumstances (e.g. when it is established that there is no other way to determine identity where it is critical to avert imminent loss of human life). Legal protections in many jurisdictions reflect this.
- Follow the principles focused on your own digital safety and security practices to avoid inadvertently causing the unmasking of your confidential source or whistleblower.
- Recognise that even if you operate to the highest standards of digital security you may not be able to protect a confidential source from identification. The objective is to be as proactive as possible and as transparent as appropriate with your source.

Anonymity at risk

Some countries have sought to criminalise anonymity online – a response to terrorism threats and cyber harassment that is finding broader traction. But the problem with 'real name conventions' is that they can chill the willingness of whistleblowers and sources to reveal important information in the public interest via communications with journalists, or through direct publication. They can also inhibit the internationally recognised human right to privacy on which journalists can potentially rely to defend their confidential communications with sources. It is therefore wise for journalists and news publishers to defend the right to anonymity in addition to protecting the identity of their own confidential sources and whistleblowers.

Exception to the rule

In very rare circumstances the ethical decision might actually be to name a person requesting anonymity. In the case of legitimate whistleblowers or confidential sources this would normally be in accordance with the narrowest of exceptions to protections. However, the more recent phenomenon of attempts by faux sources to mislead and discredit journalists by providing deliberately false information also requires consideration.

For example, in 2017 The *Washington Post* decided to identify a deceptive 'confidential source' seeking to entrap the Post in a politically-motivated false story. As the Post reported, "A woman who falsely claimed to The *Washington Post* that Roy Moore, the Republican U.S. Senate candidate in Alabama, impregnated her as a teenager appears to work with an organization that uses deceptive tactics to secretly record conversations

in an effort to embarrass its targets."[16] In this case, verification and investigative reporting processes identified the woman as a 'fake source' engaged in disinformation campaigns and the *Post* concluded (appropriately) that it was in the public interest to identify her in the context of reporting on the group she was collaborating with. Deliberate deception on the part of a confidential 'source' or faux whistleblower can occasionally justify exposure.

Case study

James Risen is a former *New York Times* National Security Editor and CIA correspondent who is now Senior National Security Correspondent at The Intercept and Director of First Look Media's Press Freedom Defense Fund. On pain of jail, during legal proceedings brought by the US Government, he refused to identify the source of information contained within his 2006 book *State of War* about a bungled covert CIA operation involving Iran. His commitment to source confidentiality and investigative journalism dependent upon whistleblowers acting in the public interest also led him into conflict with *New York Times*' management who had refused to publish the story (later told in his book) that became the subject of a 10-year legal battle.[17] Ultimately, Risen avoided jail after the US Attorney General intervened in the case. But the Obama government successfully prosecuted the man they believed to be the whistleblower at the heart of the story, Jeffrey Sterling. Risen has never confirmed if Sterling was his source, but the former CIA agent served two years in jail regardless, after the prosecution accessed Risen's email metadata.[18] To some observers, this was proof that compelling testimony from reporters may no longer be necessary to reveal a confidential source. This case demonstrates both the importance of exercising 'reporter's privilege' – a journalist's ethical and (in many countries) legal right to refuse to divulge the name of a source – and the Digital Age threats effectively eroding this core tenet of investigative journalism.

Relevant legal concepts and standards[19]

In many jurisdictions there are explicit provisions on the confidentiality of sources. For example, in the United Kingdom[20], no court may require a person to disclose, nor is the person guilty of contempt of court for refusing to disclose, the source, information relevant to a publication for which she or he is responsible, unless it can be established to the satisfaction of the court that disclosure is necessary in the interests of justice or national security, or for the prevention of disorder or crime.

The European Convention on Human Rights (ECHR), provides for the freedom to receive and impart information and ideas without interference by a public authority[21]. It was observed by the European Court of Human Rights in Goodwin v. the United Kingdom[22] that,

> *"Protection of journalistic sources is one of the basic conditions for press freedom. ... Without such protection, sources may be deterred from assisting the press in informing the public on matters of public interest. As a result the vital public-watchdog role of the press may be undermined, and the ability of the press to provide accurate and reliable information be adversely affected. ... [A]n order of source disclosure ... cannot be compatible with Article 10 of the Convention unless it is justified by an overriding requirement in the public interest."*

In France, the Code of Criminal Procedure[23] provides that any journalist who appears as a witness concerning information gathered by her/him in the course of their journalistic activity is free not to disclose its source. Germany's Civil Procedure Code[24] acknowledges that when facts are confided to persons because of their profession, including journalism, these persons are entitled to refuse to give testimony on these facts unless their source consents to disclosure. Similarly, the Criminal Procedure Code[25] authorizes radio and print journalists to refuse to testify about the content or source of information given in confidence.

Under Swedish law, a source who provides information to a journalist on condition of anonymity is protected.[26] This protection however does not apply in cases of high treason, espionage or wrongful release of an official document.[27] A journalist who, either through negligence or by deliberate intent, reveals the identity of a source may be subject to a prison sentence of up to one year, or ordered to pay a fine.[28]

In Canada, the Journalistic Source Protection Act 2017[29] provides journalists with the right to refuse to disclose information or documents that may identify a source who has requested anonymity.

In India, Freedom of Press is recognized by the Supreme Court of India as emanating from the Freedom of Speech and Expression[30]. The Press Council Act 1978, provides that no newspaper, news agency, editor or journalist will be compelled to disclose the source of any news or information published or reported by them to the Press Council of India (PCI). This provision however is only in respect of the PCI which is a statutory, self-regulatory body. Despite recommendations from the Indian Law Commission to broaden the scope of this protection there is no law which specifically protects the sources of information disclosed to journalists.

Principle 2: Provide safer ways for sources to make 'first contact' with you, where possible

Sources have to share the responsibility with us, they have to believe in the cause they're trying to promote, and it should be a shared responsibility. Both a source, or a whistle-blower, and a journalist are aiming for the same thing; expose the wrongdoings and corruption as well as promote good governance

Rana Sabbagh, Executive Director Arab Reporters for Investigative Journalism [31]

Putting this into practice

- Making first contact is frequently the way a journalist and a whistleblower can be linked in a later investigation, even if they both use encryption. An assurance of confidentiality is not the same as anonymity. Evidence of contact can be dangerous.
- Recognise that in order to share the responsibility for confidentiality, sources and whistleblowers need to be aware of the threats and be equipped to mitigate the risk.
- Help potential whistleblowers by publicising ways they can contact you using anonymised and encrypted channels[32], and the risks associated with each.
- You can give a whistleblower the chance to make first contact without leaving a trail of electronic breadcrumbs by providing a Ricochet[33] address in your public contact details, as well as announcing in advance when you will be at public events in person.
- Commit to reporting on the broad implications of privacy threats in the Digital Age, including as they pertain to undermining the public's right to know by compromising source confidentiality.

Relevant legal concepts and standards

Journalists are subject to the law of the land, implementing best practices to store, process and publish information which is collected from whistleblowers. Inversely, it is also important to exercise, proper data security so that information they have acquired is safe and secure.

It must be kept in mind that whistleblowers sometimes risk their lives by divulging confidential information to journalists. Therefore, it is the ethical obligation of the journalist to exercise good security practices and to hold data in utmost confidence, unless and until it is necessary to publish.

Principle 3: Recognise the costs of whistleblowing for the whistle-blower, and prompt them to think through ahead of time how to cope when the story breaks

> **"There are very few news organisations that will do anything about it if a source gets arrested." James Risen**

Investigative journalism that relies on whistleblowers and confidential sources is often high risk for the journalist and the publisher. But the impacts of blowing the whistle can be devastating for the whistleblower – financially, legally, professionally, psychologically, and even physically. The threats of mass surveillance and national security overreach to confidential source-dependent investigative journalism are very significant in liberal democracies but the consequences of exposure can be much more serious in fragile states and conflict zones. Impacts on whistleblowers (and, in some cases, journalists) in these environments can involve physical assault, torture and even death. The escalation of the risk of exposure in the Digital Age requires a reassessment of the consequences and costs for confidential sources and whistleblowers.

Putting this into practice

- Treat the whistleblower or confidential source you're working with in the manner they deserve - with dignity and respect, as a person taking a significant risk to entrust you with their secrets and their identity in an effort to reveal information in the public interest.
- Consider your responsibilities and your publisher's responsibilities for securing the safety and legal defence of your confidential source.
- Discuss the story and the risks to your source and with your editors early in the reporting process where you think there may be legal risks involved for you, the publisher or the source.

Relevant legal concepts and standards

There are various risks to be considered by the potential whistleblower, the most obvious being loss of their job and reputation. Balancing personal interests with public ones is a significant issue for any individual considering blowing the whistle. The prospect of legal proceedings being initiated, physical or workplace retaliation are some of the major risks whistleblowers have to consider in different jurisdictions. Physical attacks on whistleblowers are on the rise in some countries.

Principle 4: Verify material focusing on the public interest value of the information, not on your view of the attitudes or opinions of the source or whistleblower

Many sources have an agenda and whistleblowers may have a clear idea of what they want to achieve with a disclosure. However, it is the quality and verifiability of information supplied that is important in terms of judging the value of a source to public interest journalism, not the personality or politics of the individual or group supplying the information.

Putting this into practice

- Don't dismiss information supplied by a source because you disagree with their motive, philosophies, attitudes or public statements.
- While judging the information supplied on merit, it remains important to assess the motivation of the confidential source or whistleblower to determine veracity – is there malicious intent? Could there be inaccuracies secreted in the dataset, for example? [34] [35] [36]
- Ensure you apply the same standards of pre-publication verification to the information provided by a confidential source as you would to any data or witness account.

Relevant legal concepts and standards

Legal definitions of the public interest vary between jurisdictions. Under India's Whistleblower Protection Act 2014, a public interest disclosure is a complaint relating to commission of an act of corruption, wilful misuse of power or discretion by which there is loss caused to the Government or wrongful gain has accrued to a third party, and the commission or attempt to commit a criminal offence.[37] This is a relatively narrow definition in comparison to the UK's Public Interest Disclosure Act 1998, where a disclosure of information can be in relation to a criminal offence, failure to comply with any legal obligation, miscarriage of justice, health or safety of an individual is in danger, or where information is being deliberately concealed.[38]

Principle 5: Take responsibility for your digital defence and use encryption. Even though encryption may not completely defend your source, it offers important first-line protection.[39]

> **Encryption and anonymity, today's leading vehicles for online security, provide individuals with a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organizations...and others to exercise the rights to freedom of opinion and expression**
>
> **Prof. David Kaye, UN Special Rapporteur on the Promotion of Freedom of Opinion and Expression** [40]

The Digital Age presents new and very significant challenges to the ethical and legal frameworks supporting source confidentiality and the privacy of communications between journalists and whistleblowers. The costs and consequences of exposure make it incumbent upon journalists and news publishers to actively engage with these issues, raise awareness and adapt practice accordingly.

Putting this into practice

- Recognise that encryption defends press freedom through support for the privacy of confidential digital communications with sources and whistleblowers. While encryption is a minimum standard, it is not a guarantee of confidentiality. For example, digital data trails, including mobile phone geolocation information captured when meeting a source face-to-face, can lead to discovery of the source's identity.
- Use appropriate levels of encryption for digital communication (email, smartphone app etc) with confidential sources and whistleblowers, according to the identified risk factors.
- Model good practice for other journalists in this regard.
- Avoid uncritically accepting and reporting anti-terrorism or national security narratives used to justify encryption overrides and associated privacy breaches that undermine investigative journalism.

Case study: Eight tips for better digital source protection

Drawing on research conducted by the authors for this project and newsroom training developed to address source protection erosion, here are eight simple tips you can put into practice right now to better protect whistleblowers and confidential sources:

1. Decide when to use analogue era practices:
   - Meet face to face.
   - Stay off the phone, email and social media.
   - Vary your patterns of contact and meeting points.
2. Leave your smartphone behind when you meet your source (especially if your adversary is a security organisation) and tell your source to do the same.
3. In countries with ubiquitous video surveillance, you need to be cautious about meeting in areas under scrutiny.
4. Install a simple encrypted messaging app like Signal (Hint: not all encrypted apps are created equal) to communicate electronically with your source or whistleblower and get them to do the same.
5. Keep your software updated. Don't ignore those pesky verified software vendor demands to 'update', they frequently include patches to fix glitches or security flaws that might leave your/your source exposed.
6. Make your passwords long, unique and complex (try a password manager), and activate two factor authentication on all your devices or accounts.
7. Stretch timelines: If your source is at risk, it might help to put a gap between your contact with them and publication of the information they supplied.
8. Develop a plausibly-deniable backstory to explain your contact with the source/whistleblower (e.g. if your children both play football, perhaps that's why you were in the same park at the same time?).

Relevant legal concepts and standards

Encryption is the transformation of data by the use of cryptography to ensure its confidentiality.[41] In the European Union, under GDPR, it is required that technical and organizational measures are to be adopted which specifically include encryption.[42] Even where a breach of personal data is likely to result in a high risk to the rights and freedom of natural persons, if methods like encryption are adopted, then there is no requirement to communicate the breach to the data subject.[43] Thus under GDPR, encryption is cited as an important measure to mitigate the risk of any security breach.[44]

Principle 6: Determine the biggest threats to you and your source, and what specific steps you need to take to protect both of you

> **There is no one-size-fits-all security. Threat modelling is a general approach to thinking through your security needs and coming up with a plan that suits your unique circumstance**
>
> **Jonathan Stray, Journalist and Data Scientist[45]**

Before embarking upon a story or investigation involving a confidential source or whistleblower, it is important to conduct a 'risk' or 'threat' assessment applied to both the adversary and the potential consequences of your source's exposure.[46]

A risk assessment typically involves considering (in combination):

- The risks of exposure (to both the source or whistleblower and your communications with them).
- The seriousness of the potential consequences of exposure to the whistleblower or confidential source (and potentially the journalist).
- The level of threat or source identification capability posed by the organisation or individual invested in keeping the information hidden.
- The public interest value of the information.
- The defensive tactics you need to deploy in response to the above risks/threats.

Putting this into practice

- Conduct a risk assessment on every story involving a confidential source or whistleblower - in terms of both the adversary and the potential consequences of your source's exposure.[26]
- Consider when to use 'analogue era' communications practices like face-to-face meetings.
- Work to ensure your confidential sources have access to tools and training to defend their anonymity/privacy and confidentiality of communications with you.
- Establish contact with and regularly consult a range of digital security and digital safety experts to ensure you are as up to date as possible with both Digital Age risks and threats.
- Make use of organisations like The Signals Network[47] which seeks to facilitate relationships between whistleblowers, journalists, security experts, and specialist lawyers.

Relevant legal concepts and standards

The European Union's General Data Protection Regulation (GDPR) provides guidance for how personal information should be stored and used internally. Where data processing is likely to result in a high risk to the rights and freedoms of natural persons, an assessment of the impact of the envisaged processing must be carried out.[48] This impact assessment would have to take into account, inter alia, the necessity and proportionality of the processing in relation to its purposes as well as the measures envisaged to address risks, including safeguards, security measures and mechanisms to ensure the protection of personal data.[49]

Principle 7: Explain the risks of digital exposure to your source or whistleblower. On sensitive stories, train your whistleblowers in basic digital security

> **I think we're literally going back to that age, when the only safe thing is face-to-face contact, brown envelopes, and meetings in parks.**
>
> **Alan Rusbridger, Chair of the Reuters Institute for the Study of Journalism and former Editor-in-Chief of The Guardian.** [50]

While you want to avoid unnecessarily frightening off your confidential source or whistleblower, it is important to ensure that they are aware of the risks of exposure connected with digital communications (e.g. mass surveillance, metadata handover) so that they can make more secure contact with you and avoid exposing themselves inadvertently. Remember: few whistleblowers or confidential sources have the digital security skills of Edward Snowden, or 'John Doe' of Panama Papers fame.

Putting this into practice

- Explain the risks of digital communication in terms of interception, mass surveillance, targetted surveillance and metadata handover.
- Explain the fundamentals of encryption.
- Consider sharing resources outlining defensive techniques to support their self-directed learning.
- On high risk stories consider working with whistleblowers on the development of their digital defence skills.

Relevant legal concepts and standards

UNESCO's 2017 study "Protecting Journalism Sources in the Digital Age" [51] documents the contemporary risks and threats that are undermining legal and regulatory source protection. Meanwhile, UNESCO's 2016 publication on "Human rights and encryption" stated that, "from a human rights perspective, there is a growing awareness that encryption is an important piece of the puzzle for realizing a free open and trustworthy internet ... There is recognition of "the role that anonymity and encryption can play as enablers of privacy protection and freedom of expression".[52]

However, the notion of encryption as an enabler for freedom of expression is not always reflected in national laws. Legislation in many countries allows governments to access, or compel assistance to access, encrypted data for specific reasons. India's Information Technology Act 2000, for instance, empowers the Government of India and state governments to get assistance from any "subscriber or intermediary or any person in charge of the computer resource" in intercepting, monitoring or decrypting information which is generated, transmitted, received or stored in any computer resource[53] for specific national interests which include, inter alia, sovereignty or integrity of India, defence of India and security of the State.

Principle 8: Publish original documents and datasets in their entirety where possible *and* safe to do so, recognising the importance of datasets in stories

Investigative journalism in the Digital Age has been greatly assisted by the ability of sources and whistleblowers to provide source material at scale. Journalism based on sets of data, rather than individual documents – like the Snowden revelations or the Panama Papers – has the ability to shed light on entire systems and how they have evolved over time. Technology allows vast amounts of information to be understood in new ways, with statistical analysis and visualisation. Patterns and anomalies are revealed. Where the scale of a disclosure would be overwhelming for one media organization to handle, international collaborations have highlighted a range of geographical perspectives. When databases of source material are made available to researchers and the public at large, they can become part of the historical record and continue to generate insights and inform reporting for years to come. But be aware that there are digital safety risks entailed where identifying data exists within document sets - for example, microdots from a printer appear to have led to the identification of Reality Winner (a case study discussed elsewhere in this document).

Putting this into practice

- Recognise that the publication of source material makes a significant contribution to the impact of reporting.
- Use statistical and data visualisation techniques that allow readers to understand the significance of an entire dataset.
- Be open to international and other collaborations around datasets too large for one organization to handle comprehensively, or where data has a global significance that would benefit from a range of international perspectives.
- Make searchable archives of source material available to the public wherever possible, and as an integral part of your publication plan.
- Be aware of risks (e.g. inadvertent source exposure) entailed in publishing original datasets and work to mitigate them (see Principle 10 below).

Relevant legal concepts and standards

Dataset Journalism is pushing the boundaries, and often the law has yet to catch up in protecting this type of reporting. For example, in India, there is strict legal prohibition against publishing any document which may relate to a matter the disclosure of which is likely to affect the sovereignty and integrity of India, the security of the State or friendly relations with foreign States. This prohibition also extends to obtaining, collecting, recording or communicating any such document. The Official Secrets Act 1923 (OSA) governs such acts and prescribes severe punishment for contravention of its provisions which include imprisonment for a term which may extend from three years to fourteen years.[54] OSA further prohibits any person to wilfully communicate to any unauthorized person any document which he may have received or entrusted in confidence to him owing to his position in the Government or which relates to a matter the disclosure of which is likely to affect the sovereignty and integrity of India, the security of the State or friendly relations with foreign States[55]. Even though whistleblowers are protected from prosecution under OSA if they make a disclosure under WBP[56], this protection however, would not cover whistleblowers who make disclosures to journalists.

Similar laws exist in many other jurisdictions. There may also be civil liabilities incurred for publishing original documents or datasets.[57]

Principle 9: Securely delete data provided by sources, when asked, to protect the sources, consistent with ethical, legal and employer obligations

One of the risks run by whistleblowers and sources is that the documents they supply to demonstrate their case might also identify them should they fall into the wrong hands. Whistleblowers like Reality Winner and Sarah Tisdall[58] were identified from the documents they disclosed. Journalists should be aware of these factors and, where it is consistent with ethical, legal and workplace obligations, respect their sources' wishes to delete identifying or otherwise sensitive data and do so in a technically effective way.

Putting this into practice

- Be aware that documents and their metadata can be used to identify a source. Investigate ways of securely erasing, or scrubbing, metadata from documents and be cautious of who they are shared with.
- Always encrypt data entrusted to you, for example on your computer's hard drive or a portable device such as USB or phone, in order to mitigate the risks of it falling into the wrong hands.
- Understand that deleting data within your operating system (e.g. by putting a file in the Recycling Bin and then emptying it) or even reformatting a hard drive means that it may still be recoverable.
- Where necessary, seek technical advice for secure erasure that overwrites the data you want to delete to make sure it cannot be recovered.
- For higher risk information, you may need to destroy the storage device to ensure deletion.
- Use full disk encryption; you may have to actively turn this on for some devices

Relevant legal concepts and standards

Under the GDPR, data is not to be kept for longer than necessary for purposes for which the personal data was processed.[59] An exact time frame is not imposed but it may cause data processors and controllers to implement stricter requirements to delete and destroy data which is no longer deemed necessary. Further, it must be demonstrated that the data subject has consented to processing of his/her data. Consent must be specific, informed and there must be some form of clear affirmative action[60].

However, it is also stipulated in the GDPR that the rules governing freedom of expression and information, including journalistic expression should be reconciled with the right to the protection of personal data. Therefore, many provisions of GDPR have been exempted for processing which is carried out for journalistic purposes if they are necessary to reconcile the right to the protection of personal data with the freedom of expression and information[61].

Principle 10: Ensure any digital drop boxes for sources and whistle-blowers offer a good level of security, and, for higher-risk materials, anonymity

One of the most important digital tools for investigative journalism is the encrypted digital drop box, which provides sources a way of submitting documents enabling a range of important public-interest material to reach the public domain. These channels require some technical expertise to use for both publications and sources but are increasingly being adopted by news organizations, civil society and government.

Putting this into practice

- Some digital drop boxes allow sources to send documents to journalists, and continue communicating with them, without revealing their identity. They may make use of the Tor network, or a dedicated operating system.
- There are a number of drop box systems available. SecureDrop[62], and the GlobaLeaks platform[63] are used by a number of media and civil society organizations internationally.
- Secure drop box systems require some technical expertise to install, maintain and operate. Some companies, such as Whispli, also offer these services.
- It is good practice to provide clear instructions for potential sources about how to use your drop box securely and the potential risks of doing so. This could include publishing explanatory notes or videos on your website.

Relevant legal concepts and standards

Under the GDPR, personal data shall be processed in a manner that ensures appropriate security that data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, by using appropriate technical or organizational measures.[64] The controller must implement a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measure for ensuring the security of processing.[65]

At present, there are no legal provisions which would ensure that digital drop boxes for sources and whistleblowers provide a good level of security and, for higher-risk materials, anonymity. But journalists should implement all reasonable security practices and procedures with respect to the storage of data.

Principle 11: Understand the country, regional and international legal and regulatory frameworks for protecting confidential sources and whistleblowers

Source and whistleblower protections rest upon a core right to freedom of expression. Article 19 of the Universal Declaration of Human Rights guarantees the right to seek, receive and impart information and ideas through any media, and regardless of frontiers. The International Covenant on Civil and Political Rights enshrines the same rights in its article 19, which emphasizes that the freedom applies to information and ideas of all kinds. Sources and whistleblowers enjoy the right to impart information, but their legal protection when publicly disclosing information rests especially on the public's right to receive it.

Prof. David Kaye, UN Special Rapporteur on the Promotion of Freedom of Opinion and Expression[66]

Putting this into practice

- Familiarise yourself with the source protection and whistleblower laws in your country and region (e.g. European Union).
- Familiarise yourself with international covenants, declarations and resolutions that might aid your defence of source confidentiality (e.g. UN resolutions and declarations).
- Leverage these protections in your dealings with officials seeking to interfere with your rights.
- Understand that at the UN level, it is accepted that the rights that apply offline, also apply online.[67]
- Recognise the potential value of international, regional and local laws covering source protection and whistleblowing in legal action targeting you or your sources.
- Assess your own country's legal and regulatory framework protecting confidential sources and whistleblowers against UNESCO's 11-point model[68] (See Appendix 2) and identify or report on the gaps that need addressing.

Relevant legal concepts and standards

Whistleblower protection laws vary greatly between jurisdictions. For a global overview, see Blueprint for Free Speech's Analysis of Whistleblower Protection Laws.[69]

Principle 12: Encourage news publishers to practice their responsibility to provide proper data security for journalists, sources and stored materials, along with appropriate training and policies to guide journalists

> **I didn't realise how much things had changed since I was investigating terrorist networks. My young reporters are living through different times and I now see my advice might have been out of date**
>
> **Maria Ressa – Executive Editor and CEO, Rappler.com[70]**

Digital Age threats, risks, and opportunities have dramatically altered investigative journalism over the past decade. While it is now possible to leak masses of data to journalists on an unprecedented scale, there is a parallel threat of digital discovery confronting both whistleblowers and journalists. This threat must be countered if investigative journalism dependent upon confidential sources is able to be conducted effectively in the Digital Age.

Putting this into practice

- If you work for a news organisation, highlight the Digital Age risks affecting communications with confidential sources and whistleblowers to your superiors.
- Insist on appropriate training to improve your digital defences.
- Insist on the adoption of newsroom policies and guidelines for dealing with confidential sources and whistleblowers in the Digital Age for wide dissemination within the organisation (recognising that a weak link in the newsroom chain could compromise a confidential source or whistleblower).
- Highlight the legal and editorial threats of complacency on these issues to your employers or editors.
- If you are an editor or publisher, recognise and respond appropriately to the risks raised above.
- Ensure that your organisation has an appropriately integrated strategy for defending digital security that recognises the implications for confidential communications with sources and whistleblowers (i.e. there is a need for a holistic approach that integrates analogue safety, digital security, legal policy and training).
- If you are a freelance journalist, contact your trade union or an NGO working in this space (e.g. Blueprint for Free Speech or The Signals Network) for assistance.
- Consider training whistleblowers in the basics of secure digital communications.

Relevant legal concepts and standards

Whistleblowers in the Digital Age are vulnerable to new types of legal sanctions, including computer crime laws. These typically do not have any kind of journalistic exemption or public interest defence. This new kind of risk underlines the importance of journalists raising the data security standards across their profession.

Resources to help you implement these guidelines

Open Access Books and Reports

Cannataci, J, Zhao, B et al (2016) Privacy, free expression and transparency: Redefining their new boundaries in the digital age (UNESCO) Available at: http://unesdoc.unesco.org/images/0024/002466/246610e.pdf

GAP (2017) Working with Whistleblowers: a guide for journalists. Available at: http://www.whistleblower.org/sites/default/files/whistleblowerguidejournalism.pdf

Henrichsen J, Lizosky J & Betz, M (2015) Building Digital Safety for Journalists (UNESCO: Paris). Available: http://unesdoc.unesco.org/images/0023/002323/232358e.pdf

Kaye, D (2015) UN Special Rapporteur Report on Encryption, Anonymity and the Freedom of Expression (UN General Assembly). Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement

Kaye, D (2015) Selected References: Unofficial Companion to Report of the Special Rapporteur (A/HRC/29/32) on Encryption, Anonymity and the Freedom of Expression. Available at: https://www.ohchr.org/Documents/Issues/Opinion/Communications/States/Selected_References_SR_Report.pdf

Kaye, D (2015) Report of the Special Rapporteur to the General Assembly on the Protection of Sources and Whistleblowers. Available at: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/361

Kaye, D (2018) Encryption and Anonymity Follow-up Report, UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (UN Office of the High Commissioner on Human Rights). Available at: https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf

Open Societies Foundation (2013) The Global Principles on National Security and the Right to Information (the Tshwane Principles). Available at: https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf

Posetti,J (2017) Protecting Journalism Sources in the Digital Age (UNESCO: Paris). Available at: http://unesdoc.unesco.org/images/0024/002480/248054E.pdf

Ramos,J G (2016) Journalist Security in the Digital World: A Survey (CIMA). Available at: https://www.cima.ned.org/wp-content/uploads/2016/03/CIMA-Journalist-Digital-Tools-03-01-15.pdf

Schulz, W & van Hoboken, J (2016) Human Rights and Encryption (UNESCO). Available at: http://unesdoc.unesco.org/images/0024/002465/246527E.pdf

Websites

Blueprint for Free Speech: https://blueprintforfreespeech.net/

The Signals Network: https://thesignalsnetwork.org/

APPENDIX 1

Perugia Principles Expert Advisory Panel*
Natalia Anteleva – Coda Story
Peter Bale – Board member, The Signals Network
Joyce Barnathan – International Center for Journalists (ICFJ)
Caelain Barr – *The Guardian*
Daniel Howden – Refugees Deeply
Cherilyn Ireton – World Editors Forum
Joel Konopo – INK
Jeff Larson - Pro Publica
Caroline Lees – Reuters Institute for the Study of Journalism (RISJ)
Jean Paul Marthoz – *Le Soir*
Rosa Meneses - *El Mundo*
Ntibinyane Ntibinyane – INK
Kristina Ozimec – Platform for Investigative Journalism and Analysis (PINA)
Ernst Jan Pfauth – De Correspondent
Courtney Radsch – Committee to Protect Journalists
Maria Ressa – Rappler.com
James Risen – The Intercept
Bruce Shapiro – Global Investigative Journalism Network (GIJN)/Dart Center for Journalism and Trauma
Declan Walsh – *New York Times*

*All affiliations were correct at the time of participation

APPENDIX 2

UNESCO's Model Legal Source Protection Framework[71]

1. Recognise the value to the public interest of source confidentiality protection, with its legal foundation in the right to freedom of expression (including press freedom), and to privacy. These protections should also be embedded within a country's constitution and/or national law,

2. Recognise that source protection should extend to all acts of journalism, and across all platforms, services and mediums (of data storage and publication), and that it includes digital data and meta-data,

3. Recognise that source protection does not entail registration or licensing of practitioners of journalism,

4. Recognise the potential detrimental impact on public interest journalism, and on society, of source-related information being caught up in bulk data recording, tracking, storage and collection,

5. Affirm that State and corporate actors (including third party intermediaries) who capture journalistic digital data must treat it confidentially (acknowledging also the desirability of the storage and use of such data being consistent with the general right to privacy),

6. Shield acts of journalism from targeted surveillance, data retention and handover of material connected to confidential sources,

7. Define exceptions to all the above very narrowly, so as to preserve the principle of source protection as the effective norm and standard,

8. Define exceptions as needing to conform to a provision of "necessity" and "proportionality" — in other words, when no alternative to disclosure is possible, when there is greater public interest in disclosure than in protection, and when the terms and extent of disclosure still preserve confidentiality as much as possible,

9. Define a transparent and independent judicial process with appeal potential for authorised exceptions, and ensure that law-enforcement agents and judicial actors are educated about the principles involved,

10. Criminalise arbitrary, unauthorised and wilful violations of confidentiality of sources by third party actors,

11. Recognise that source protection laws can be strengthened by complementary whistle-blower legislation.

Endnotes

1 James Risen was interviewed by Julie Posetti during the International Journalism Festival in Perugia, Italy, in April 2018

2 See: International Federation of Journalists' (IFJ) Declaration of Principles on the Conduct of Journalists available here: https://www.ifj.org/who/rules-and-policy/principles-on-conduct-of-journalism.html

3 See: Thematic Study 2 in *Protecting Journalism Sources in the Digital Age* (Posetti 2017: 112-120)

4 Protecting Journalism Sources in the Digital Age (Posetti 2017) is a comprehensive UNESCO-commissioned study of the state of legal and normative source protection frameworks in 121 countries written by the co-author of these guidelines. It is a recommended resource for journalists, news organisations, media lawyers, and NGOs dealing with press freedom issues and whistleblower protection. It is freely available here: http://unesdoc.unesco.org/images/0024/002480/248054E.pdf

5 Ibid, p. 18

6 Ibid, p. 7

7 See: Ireton C & Posetti J (2018) Journalism, Fake News and Disinformation (UNESCO: Paris) Available here: http://unesdoc.unesco.org/images/0026/002655/265552e.pdf.

8 Posetti, J (2017) Op Cit p104

9 Gallagher, S (2017) How a few yellow dots burned the Intercept's NSA leaker, *Arts Technica*: https://arstechnica.com/information-technology/2017/06/how-a-few-yellow-dots-burned-the-intercepts-nsa-leaker/ [Accessed 24/10/18]

10 Sullivan, M (2017) The Intercept failed to shield its confidential source, now it's making amends, *The Washington Post*: https://www.washingtonpost.com/lifestyle/style/the-intercept-failed-to-shield-its-confidential-source-now-its-making-amends/2017/07/11/9d41284a-65d8-11e7-8eb5-cbccc2e7bfbf_story.html?noredirect=on&utm_term=.5133397bfe01 [Accessed 24/10/18]

11 See: Signal Messenger, https://signal.org

12 Radsch, C. C. (2016) Cyberactivism and Citizen Journalism in Egypt: Digital Dissidence and Political Change (New York: Palgrave Macmillan) p. 24] leading to the identification of confidential sources

13 A 'research roundtable' of expert contributors was facilitated by Julie Posetti in connection with this project during the International Journalism Festival in Italy on April 14th, 2018. Twenty international investigative journalists, press freedom experts and digital security specialists participated. Their contributions have helped shape this set of principles and guidelines. Participants in this research who chose to be identified are listed in Appendix 1.

14 Nishith Desai Associates

15 Posetti, J (2018) Working with Whistleblowers in the Digital Age: New Guidelines, European Journalism Observatory. Available at: https://en.ejo.ch/specialist-journalism/working-with-whistleblowers-in-the-digital-age (Accessed 1/12/18)],

16 Boburg, S et al (2017) "A woman approached The Post with dramatic — and false — tale about Roy Moore. She appears to be part of undercover sting operation", *The Washington Post*. Available here: https://www.washingtonpost.com/investigations/a-woman-approached-the-post-with-dramatic--and-false--tale-about-roy-moore-sje-appears-to-be-part-of-undercover-sting-operation/2017/11/27/0c2e335a-cfb6-11e7-9d3a-bcbe2af58c3a_story.html?utm_term=.e7e3af004b9c

17 Risen, J (2018) The Biggest Secret: My life as a New York Times reporter in the shadow of the War on Terror, *The Intercept*: https://theintercept.com/2018/01/03/my-life-as-a-new-york-times-reporter-in-the-shadow-of-the-war-on-terror/ [Accessed 30/4/18]

18 Mass, P (2018) Jeffrey Sterling: Convicted of leaking about botched CIA program, released from prison, *The Intercept*: https://theintercept.com/2018/01/19/jeffrey-sterling-cia-leaking-prison/ [Accessed 28/8/18]

19 In particular, the authors thank Rahul Rishi, Aaron Kamath and Inika Charles (Nishith Desai Associates), and give special acknowledgement to Maryam Naaz Quadri (Faculty of Law, Delhi University)..
20 Section 10 of the *Contempt of Court Act 1981*, United Kingdom
21 Article 10 of the *European Convention of Human Rights*
22 1996) 22 EHRR 123 see para 39, *Goodwin v. the United Kingdom*
23 Article 109(2) of *France Code of Criminal Procedure*
24 Section 383 of *Germany's Civil Procedure Code*
25 Section 53 of *Germany's Criminal Procedure Code*
26 Chapter 3, *Freedom of the Press Act*, Sweden
27 Chapter 5, Article 3, *The Fundamental Law on Freedom of Expression*, Sweden
28 Ibid, Chapter 2, Article 5
29 Section 39.1 (2) of *Journalistic Source Protection Act 2017*, Canada
30 Article 19(1)(a) of the *Constitution of India* 31 Posetti , p 111
32 See: https://blueprintforfreespeech.net/en/free_speech_software/
33 Ibid
34 See Shafer, J (2018) "No, Amy Chozick, You're Not a Russian Agent", *Politico Magazine*, https://www.politico.com/magazine/story/2018/04/25/no-amy-chozick-youre-not-a-russian-agent-218075
35 See: Shane, S (2018) "When Spies Hack Journalism", *The New York Times*: https://www.nytimes.com/2018/05/12/sunday-review/when-spies-hack-journalism.html
36 See also this video discussion on the theme from the International Journalism Festival in 2018: How to report on Hacks, Leaks and Data Breaches: https://www.youtube.com/watch?v=-F07LrSVpg6Q
37 Section 3(d) of *Whistleblower Protection Act 2014*, India
38 Section 43B of *Public Interest Disclosure Act 1998*, United Kingdom
39 Encryption can keep your communications confidential. However it doesn't provide anonymity, so your source may still be identified via digital metadata trails even if you use encryption. Endpoint security is also important; if your phone's security is compromised, encrypted messaging isn't going to keep any chats with your source confidential.
40 Kaye, D (2015) UN Special Rapporteur Report on Encryption, Anonymity and the Freedom of Expression (UN General Assembly). Available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/095/85/PDF/G1509585.pdf?OpenElement
41 Organization for Economic Co-operation and Development *Guidelines for Cryptography Policy*, OECD
42 Article 32(931)(a) of *GDPR*, European Union
43 Article 34(3)(a) of *GDPR*, European Union
44 Some internet and telecommunications companies publish transparency reports about data requests received from governments along with their responses. Journalists may wish to examine rankingdigitalrights.org (for example) to see which actors provide the most protection.
45 See this 2014 post from Jonathan Stray about how to approach 'threat modelling': https://source.opennews.org/articles/security-journalists-part-two-threat-modeling/
46 See: Henrichsen, J et al (2015) *Building Digital Safety for Journalists* (UNESCO: Paris) for guidance on conducting risk assessments and positioning stories on a 'threat hierarchy'
47 See: The Signals Network https://thesignalsnetwork.org/mission/
48 Article 34(1) of *GDPR*, European Union
49 Article 34(7) of *GDPR*, European Union
50 Posetti, 109
51 Posetti, J (2017) Protecting Journalism Sources in the Digital Age (Paris: UNESCO) Available here: http://unesdoc.unesco.org/images/0024/002480/248054E.pdf
52 See pages 10 and 11 of this handbook
53 Section 69 of *Information Technology Act 2000,* India
54 Section 3(1)(c) of *Official Secrets Act 1932*, India

55 Section 5(1) of *OSA*, India
56 Section 4(1) of *WBP*, India
57 There may be copyright implications of publishing original documents. The reproduction of an original document, could result in copyright infringement if it is done without consent, and if it is not a permitted use under the *Copyright Act, 1957,* India
58 Guardian Research Department (2011), 22 October 1983: Sarah Tisdall. Available at: https://www.theguardian.com/theguardian/from-the-archive-blog/2011/jun/03/guardian190-sarah-tisdall-1983
59 Article 5(1)(e) of *GDPR*, European Union
60 Article 7 of *GDPR*, European Union
61 Article 85 of *GDPR*, European Union
62 See :SecureDrop: https://securedrop.org/
63 See: GlobaLeaks: https://www.globaleaks.org/
64 Article 5(1)(f) of *GDPR*, European Union
65 Article 32(1)(d) of *GDPR*, European Union
66 Note: See Prof. David Kaye's Report to the General Assembly on the Protection of Sources and Whistleblowers. Available here: http://www.un.org/en/ga/search/view_doc.asp?symbol=A/70/361
67 See: See Protecting Journalism Sources in the Digital Age (UNESCO:2017) for a survey of relevant regional and international laws, agreements and regulations (esp. pp30-101). Available here: http://unesdoc.une- sco.org/images/0024/002480/248054E.pdf. See also, Thomson Reuters Foundation, Reporters Without Borders & Hastings, P (2015), Defence Handbook for Journalists and Bloggers on Freedom of Expression and Freedom of Information Principles in International Law, Thomson Reuters Foundation. Available here: http://www.trust.org/publications/i/?id=dceec155-7cb8-4860-a68e-4b463e562051
68 See: *Protecting Journalism Sources in the Digital Age* pp 120-134. Available here: http://unesdoc.unesco.org/images/0024/002480/248054E.pdf
69 See: Blueprint for Free Speech: https://blueprintforfreespeech.net/en/library-overviews/
70 Maria Ressa joined the expert advisory panel facilitated by Julie Posetti for this project at a 'round table' discussion in Perugia, Italy, in April 2018.
71 Posetti 2017, pp 132-133

NOTES


blueprint for
FREE SPEECH