The Perugia Principles for Journalism:

Working with Whistleblowers in the Digital Age

blueprint for FREE SPEECH

12 PRINCIPLES FOR WORKING WITH WHISTLEBLOWERS IN THE DIGITAL AGE

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

1

Protect your sources. Defend anonymity.

A journalist's commitment to protect the anonymity of confidential sources and whistleblowers should only be breached in the most exceptional circumstances

Focus on your own digital safety to avoid inadvertently causing the un-masking of your confidential source.

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.

blueprint for FREE SPEECH

2 Provide safer ways for sources to make 'first contact'.

First contact is frequently the means by which a journalist and a whistleblower can be linked in a later investigation, even if they both use encryption.

Help potential whistleblowers by publicising ways they can contact you using anonymised and encrypted channels. Include digital addresses, usernames or public keys in your public contact details.

Announce in advance when you will be at public events in person.

Report on the broad implications of privacy threats in the Digital Age undermining the public's right to know by compromising source confidentiality.

3

Recognise the costs of whistleblowing, help sources think through what happens when the story breaks.

Treat the person taking a significant risk to entrust you with their secrets and their identity in an effort to reveal information in the public interest with dignity and respect.

Consider your responsibilities, and your publisher's, for securing your sources safety and legal defence (where relevant).

Discuss the story and possible legal risks with your editors early in the reporting process.

blueprint for FREE SPEECH

4

Focus on the public interest value of the information, rather than the attitudes or opinions of your source.

Don't dismiss information supplied by a source because you disagree with their motive, philosophies, attitudes or public statements.

While information should be judged on its merits, it remains important to assess the motivation of your source. Be aware of the possibility of inaccuracies in datasets, including malicious ones.

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.

Take responsibility for your digital defence and use encryption.

5

Encryption defends press freedom, but it is not a guarantee of confidentiality. Digital data trails can lead to discovery of a source's identity.

Use encryption in digital communications with confidential sources and whistleblowers, but be aware of its limitations, especially where metadata is concerned.

Model good practice for other journalists in this regard.

Avoid uncritically reporting anti-terrorism or national security narratives used to justify encryption overrides and associated privacy breaches that undermine investigative journalism.

blueprint for FREE SPEECH

6

Determine the biggest threats to you and your source. Take steps to protect both of you.

Conduct a risk assessment for the story you are working on and the source you are working with.

Consider when to use analogue era communications practices like face-to-face meetings.

Make use of organisations like The Signals Network that seek to facilitate relationships between whistleblowers, journalists, security experts, and specialist lawyers.

7

Explain the risks of digital exposure to your source or whistleblower. Train your whistleblowers in basic digital security.

Explain the risks of digital communication in terms of interception, mass surveillance, targetted surveillance and metadata handover.

Make sure your source is confident with any digital tools you are using to communicate.

Explain what those tools can do and what they cannot. Help your source to understand the risks of digital communication that apply to their particular situation.

Consider sharing resources outlining defensive techniques to support your source's self-directed learning.

.

blueprint for FREE SPEECH

8

Publish original documents and datasets where possible and safe to do so.

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 large datasets, which can benefit from a range of perspectives.

Make searchable archives of source material available to the public.

Be aware of the risks entailed in publishing original datasets and work to mitigate them.

9

Securely delete data provided by sources, when asked, consistent with ethical, legal and employer obligations.

Documents and their metadata can be used to identify their source. Be cautious how and where you share them. Get technical advice.

Always encrypt data stored on your computer's hard drive or a portable device, such as a USB or phone. Turn on full-disk encryption.

Deleting data within your operating system means that it may still recoverable. Seek expert help to be sure data is securely erased so it cannot be recovered.

For high risk information, you may need to destroy the storage device to ensure deletion.

blueprint for FREE SPEECH

10

Ensure digital drop boxes offer a good level of security and anonymity.

There are a number of drop box systems available, which allow sources to send documents to journalists and continue communicating with them without revealing their identity. Most make use of the Tor network, or other such system.

Get technical advice before installing a drop box and understand what is required in order to operate and maintain it.

Provide clear instructions for sources about how to use your drop box securely and the potential risks. This could include publishing explanatory notes or videos on your website.

11

Understand the legal and regulatory frameworks for protecting confidential sources and whistleblowers.

Familiarise yourself with the source protection and whistleblower laws in your region and internationally. Understand that at the UN level rights that apply offline also apply online.

Let your source know about legal protections open to them, if they exist.

Report on efforts to secure better whistleblower protections in law.

blueprint for FREE SPEECH

12

Encourage news publishers to provide proper data security and appropriate training for journalists.

Insist on the adoption of newsroom policies and guidelines that acknowledge Digital Age threats to source protection.

Highlight the legal and editorial threats of complacency on these issues.

If you are an editor or publisher, respond appropriately to the risks.

Ensure your organisation has a strategy for defending digital security that integrates analogue safety, digital security, legal policy and training.

If you are a freelance journalist, contact your trade union or an NGO for assistance.

Acknowledgements

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, The Signals Network

Resources

BlueprintForFreeSpeech.net
TheSignalsNetwork.org
UNESCO's Protecting Journalism Sources in the Digital Age (2017)
https://en.unesco.org/unesco-series-on-internet-freedom

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 during the International Journalism Festival in Perugia, Italy in April 2018.

The authors then consulted with the broader investigative journalism, legal and academic communities to refine the Principles.

blueprint for FREE SPEECH