Issues in Investigative Practice

Proceedings of seminars at
the third international
CIJ Logan Symposium
London, 19/20 October 2018

Maria Teresa Ronderos
Matt Kennard
Rachel Oldroyd
Stephen Grey
Gabriella Coleman
Ed Moloney
Gill Phillips
Phil Chamberlain
Bill Goodwin
Julie Posetti
Chris Woods
Iona Craig
Anand Gopal
James Harkin
Eyal Weizman
Samaneh Moafi
Eliot Higgins
Sarah Giaziri
Laurent Richard
Pavla Holcova
May Jeong
Silkie Carlo
Joseph Cox
Marie Gutbub
Fabio Natali

Edited by Tom Sanderson

centre for investigative journalism

Supported by:

OPEN SOCIETY FOUNDATIONS

Introduction

Investigative Practice is a series of experimental seminars developed by The Centre for Investigative Journalism especially for the 2018 Logan Symposium: Conspiracy.

Over the course of the series invited guests and attendees were given the opportunity to learn the tools, tactics and strategies of traditional and emergent investigations; from some of the world's foremost journalists, thinkers and doers.

Each session included an expert Chair and Panel, but the discussion was open, informal and participatory, with the intention that everyone present had a chance to contribute their own perspectives and ask questions.

Each seminar lasted 60 mins and aimed to:

- Address hurdles and contradictory elements between emerging techniques and traditional practice.
- Foster interdisciplinary collaboration between journalists, hackers, academics, artists and activists in order to challenge power and investigate abuses and injustice.
- Create a network made up of people with a wide range of perspectives on the issues, from academia to professional practitioners.
- Initiate a working legacy for the Logan Symposium that records and disseminates some of the expertise brought together for the event.

Tom Sanderson

20 Oct 2018

Design: Lizzy Burt
Reporting Team:
Jenny Gunther
Nick Dowson
Matty Edwards
Olivia Church

Contents

PAGE 03

Protecting Independence: Who Pays the Piper?

Maria Teresa Ronderos
Matt Kennard
Rachel Oldroyd

PAGE 13

Winning the Trust of Sources – On and Offline

Stephen Grey
Gabriella Coleman
Ed Moloney

PAGE 20

Blowback: The Dangers of Whistleblowing – For Both Sources and Journalists

Gill Phillips
Phil Chamberlain
Bill Goodwin
Julie Posetti

PAGE 31

On the Ground and in the Ether

Chris Woods
Iona Craig
Anand Gopal

PAGE 39

Forensic Journalism

James Harkin
Eyal Weizman
Samaneh Moafi
Eliot Higgins

PAGE 50

Protecting Stories

Sarah Giaziri
Laurent Richard
Pavla Holcova
May Jeong

PAGE 58

Source Code

Silkie Carlo
Joseph Cox
Marie Gutbub
Fabio Natali

1

Protecting Independence: Who Pays the Piper?

Maria Teresa Ronderos
Matt Kennard
Rachel Oldroyd

Proceedings of seminars at
the third international
CIJ Logan Symposium

London, 19/20 October 2018

Goldsmiths, University of
London

Protecting Independence: Who Pays the Piper?

While the mainstream media withers, investigative practice is thriving, but it's easy to lose sight of who's funding it; big tech companies and philanthropic foundations, partisan NGOs and think-tanks. As investigative journalism becomes funded by practitioners outside its traditional field, are journalists still calling the tune?

In this seminar, Investigative Practice looked into the emerging new funding landscape for investigative journalism, and tackled the issues this raises for real, truth-seeking independent journalism.

Chair:

Maria Teresa Ronderos

Open Society Foundation

Panellists:

Matt Kennard

*Journalist and author of **The Racket***

Rachel Oldroyd

The Bureau of Investigative Journalism

> "There are many conspiracy theories around philanthropic funders controlling the media, but in the 4 and a half years I have worked on the Independent Journalism Programme at the Open Society Foundation, I have met George Soros only once. I introduced myself as the Director of the Programme and he said: 'Is that with us?'."
>
> Maria Teresa Ronderos

The truth lies somewhere between the extremes of total independence for funded journalism and total control from the funder.

- There are some key questions and potential problems with a philanthropically funded model of journalism.
- Does it skew the market and ultimately the angles and perspectives that journalists and stories take? Is this more or less of a problem than the model of advertisers funding journalism?
- Is there a real danger that funders alienate local communities by enforcing US and European agendas?
- There is currently a lot of philanthropic funding for technological 'fact-checking' solutions to the problem of 'fake news'. Does this risk overlooking problems with the algorithms that are intended to create the solution?
- There is also an increased drive for 'impact' when journalism is funded philanthropically. Does this result in a push towards click-bait to give favourable metrics for funding reports? Or is that necessary to ensure that journalists consider their audience and push for change?

> "All funding models are flawed, but the advertising model has the most significant flaws."
>
> Matt Kennard

Matt Kennard's experience working for places like *The Guardian* and the *FT* is that the concerns of advertisers are prioritised by editors. At *The Guardian*, they have a difficult business model because they refuse to put up a paywall, and as a result they have given sections of the website over to businesses.

Even with formal independence this has subconscious effects since editors are always aware of the interests of the funder/advertiser. Kennard has seen advertisers given a free space to respond to criticism – and would seriously question whether they would be given this space if not for the financial support.

Case study: SAB Miller

Just three days after publishing Kennard's investigation with Claire Provost which examined the multinational brewing company SAB Miller's role in damaging water security for communities in El Salvador, *The Guardian* published an 800-word interview with the Latin America division president of SAB Miller, blaming water insecurity on politics and poor infrastructure.

Kennard argues that the company's involvement in *The Guardian*'s then 'Partner Zone' scheme where corporate funding paid for content on a specific section of the website had, at least in part, an influence on the decision to publish this interview as an indirect response.

However, there are also problematic elements in foundation funding. Even in cases where a philanthropic foundation publicly promotes the aim of building independent media, their own organisational biases and agendas will still exert an influence often in indirect or unacknowledged ways. Many large foundations are quite risk averse in what they fund, which produces a chilling effect and discourages organisations, media and journalists from addressing potentially controversial subjects.

Kennard has seen instances and experienced this phenomenon when at The Centre for Investigative Journalism where organisations have been told to distance themselves from a particular issue or group by potential funders. The indirect influence that this has is clear.

The only real model which meaningfully addresses the editorial influence of funding sources is that pursued by the *Bristol Cable*, which is working towards being fully funded by membership donations and can then be democratically accountable to their membership, rather than influenced by more powerful interests, whether those are corporate advertisers, press barons, or philanthropic organisations.

> "There's a real need to turn conversations around these issues from pessimism to optimism."
>
> Rachel Oldroyd

The Bureau of Investigative Journalism is totally philanthropically funded, with an annual budget of £12 million that comes from around 13 different funders. They describe themselves as independent, but the facts are that good journalism requires resources, and therefore all journalists and media organisations are dependent to some extent on the source of those resources. The idea that there's a truly independent media model is a bit of a myth, though the model of the *Bristol Cable* is certainly an interesting one.

Most media organisations across the world are majority owned by press barons or other wealthy individuals. These people own media organisations in part because they are seeking profits, but also because they recognise that the media exerts influence, both socially and politically. This is particularly true in the 'global south'.

Although in India there is actually a growing media industry based on a traditional advertising revenue model, in the UK; in wider Europe; and certainly in America, there is a crisis of advertising. The model is completely collapsing.

Alongside this, there is also a rapidly developing crisis of trust and a proliferation of information and 'news' sites. As professional journalists, this is our industry to save and it's up to us to come up with ways to save it.

Causes for optimism

In the midst of these crises though, there are reasons for optimism. The philanthropic, not-for-profit model, while not a silver bullet, is certainly a stepping stone that can help us get to the point where we have a model that's more reflective of an independent media.

The huge drop in advertiser funding is well documented and recognised, but there's a need to acknowledge the problems that existed in the old models that are being undermined by this drop and see the opportunities that the new landscape presents. With the new plurality of models and forms, this is actually a very exciting time for investigative journalism.

One of these opportunities exists in the potential of not-for-profit philanthropically funded journalism. The not-for-profit model changes the drive, from one of maximising clicks, readers and revenue to maximising 'impact'. Despite the controversy of that term, when the currency of journalism becomes transformation rather than transaction, then the objective of providing evidence which can lead to real change becomes increasingly important. You do not see that in the commercial media space and that's an incredibly exciting model for the world in which we live.

Causes for optimism *Continued*

In China and Asia there are interesting things happening in independent media that weren't before. The majority of media organisations are increasingly aware of these questions and of the need to have a diverse range of funding sources. The Open Society Foundation aims to support the risky and controversial parts of journalism primarily, but that does mean that other media organisations need to find new models with which they can continue funding themselves.

Other funders in this sector, such as Kathryn Geels, Director of the European Journalism Centre's (EJC) Engaged Journalism Accelerator project agree with this. "The EJC sees 'impact' as the achievement of grantees' aims, rather than the EJC's own. The engaged journalism accelerator grants aim for resilience rather than sustainability, since resilience allows organisations to survive the inevitable changes in systems and adapt to take advantage of these."

It is a positive change that our media and information is no longer owned by a handful of press barons. There are a huge range of new and interesting projects happening now experimenting with a variety of different models, encompassing subscriber, membership, co-operative, collaborative and cross-disciplinary:

Collaborative, Cross-border, Cross-disciplinary

- International Consortium of Investigative Journalists (ICIJ) — The collaborative network of 220 investigative journalists in over 80 countries responsible for the Panama Papers exposé among others.
- Organised Crime and Corruption Reporting Project — Consortium of investigative centres, media organisations and journalists operating across several regions.
- Investigate Europe — Cross-border collaboration between investigative journalists from eight different european countries.
- Bureau Local — Network run by the Bureau of Investigative Journalism bringing together data journalists, local reporters and many others with diverse skills and experiences to collaborate on projects to report on issues both in regions across the UK and nationally.
- DataLEADS — organising boot-camps all over India, bringing together journalists with doctors and scientists to collaborate on data work around topics such as health and education.

Causes for optimism
Continued

Non-Profit

- The Bureau of Investigative Journalism — non-profit, foundation-funded investigative journalism outlet.
- Centre for Investigative Journalism Korea: Newstapa — funded entirely by donations from members of the public, eschewing grants from philanthropic foundations as well as businesses and government bodies.
- Correctiv — German national non-profit outlet focused on investigating injustices and abuse of power.
- Bellingcat — publishes the findings of citizen journalist investigations into war zones and the criminal underworld.
- Disclose — a new project aiming to be the first non-profit journalism in France.

Cooperatives, memberships

- The *Bristol Cable* — new model for local news delivery where the readers are the shareholders, also free media training courses for the public.
- The Ferret — non-profit investigative journalism for Scotland working on a supporter-funded model, and again training their community network in investigative skills.
- El Diario — membership-funded online newspaper, used Google start-up funding to build the software behind its member management system.
- De Correspondent — The Dutch investigative journalism outlet that crowd-funded more than €1M in just eight days during its start-up phase in 2013.
- Tortoise — Membership-funded journalism outlet dedicated to open, transparent slow news.

Causes for optimism
Continued

Subscription

- MediaPart — French non-profit investigative news organisation funded exclusively by subscription revenue from its 140,000 subscribers. Actively involves its subscribers in the news process, through Club Mediapart.
- Novara Media — Independent subscriber-funded journalism outlet self-identifying as radical left-wing.
- Real Media — Cooperative of journalists funded by individual donors and subscriptions.

There are also more and more organisations working to support the sector

- Centre for Investigative Journalism — Provides guidance, support and training for community journalism projects across the UK.
- Centre for Community Journalism — Offers networking, information and training for community journalists, and set up a representative body for the sector, The Independent Community News Network, to provide a stronger voice to champion new sustainable forms of local digital and print journalism.
- European Journalism Centre — International non-profit that runs the Engaged Journalism Accelerator, providing grant funding, mentoring and resources for innovative projects on engaged journalism.
- Membership Puzzle Project — Public research collaboration investigating methods for rebuilding trust and finding a sustainable future for public-interest journalism through membership schemes.
- Gather — Digital hub for the community of practice emerging around the concept of engaged journalism.
- The Media Fund — Co-operative working to advocate for and crowd-fund for 50 independent media partners.

Changes in methods as well as models

Other changes are also happening within the industry. Beyond experiments in new business models for journalism, new practices and working methods are also emerging from the crises that face the profession. Collaboration is becoming more and more embedded in how a lot of journalists work. This is evident in models like the ICIJ, but also in different contexts such as the Bureau Local network, which is about to be replicated in Germany by the Correctiv.Lokal project.

Changes in methods as well as models *Continued*

It's important to understand things from the perspective of local communities as well, media in the UK has traditionally been very London-centric and this can be identified as one major cause of the recent crisis of trust in journalism.

There's a need for much more collaboration and conversation not just between different organisations and different journalists, but also between journalists and their audiences. There are several examples of activities that work towards this two-way conversation.

- De Correspondent's public notebooks
- Public Newsroom at Chicago's City Bureau
- Bureau Local collaborative projects and HackDays
- HuffPost Listens project in the US and Birmingham
- *Bristol Cable*'s AGMs
- The Ferret's crowd-sourced and crowdfunded investigations

It can be argued that even the idea of what a journalist is has changed. For example, for the last couple of years Kennard has been working for NGOs. In his opinion, they are producing some of the best journalism, meaning a real democratisation of what it means to be a journalist is possible. Kennard cites Greenpeace's investigative work around the Transatlantic Trade and Investment Partnership and other trade negotiation leaks which had a major impact and in Kennard's opinion is one of the most important bits of recent journalism.

Threats and challenges

Despite the optimism, there are still downsides to the new models and methods that are emerging. It's problematic, for instance, to rely on philanthropic billionaires to fund an industry, since there's little to stop them from getting bored and moving on to the 'next new toy'.

The funding and interest is still increasing, but there's little guarantee it will last into the future, so there's an urgent need to use the current situation to find other ways to fund independent journalism that are both sustainable and resilient.

There's also a danger that a foundation-funded model will merely preserve the undemocratic hierarchical structures that currently exist. If we wish to make sure that the outcome is not just a replica of the old models, but with different sources of funding, there's also a need to genuinely embrace new ideas and models and the full potential they carry.

Threats and challenges
Continued

There's even a potential problem in the more democratic funding of membership models in outlets becoming hostage to their readerships. A major part of the role of investigative journalism has always been to challenge received wisdom and provide new perspectives which can sometimes be controversial. Is this still possible if the findings of an investigative project are unpopular with those readers who provide the funding through their membership donations?

We also need to be careful to ensure that those communities that access more influence in member-funded journalism outlets are not restricted only to the more affluent sections of society, excluding those who do not have the capacity to make regular donations.

2

Winning the Trust of Sources – On and Offline

Stephen Grey
Gabriella Coleman
Ed Moloney

Proceedings of seminars at
the third international
CIJ Logan Symposium

London, 19/20 October 2018

Goldsmiths, University of
London

Winning the Trust of Sources – On and Offline

The slow, careful art of soliciting a trustworthy source is one of the most exciting and overlooked skills in the investigative journalist's toolkit. But how does it work when the source can only be reached via digital means, or presents only an anonymous identity in the first place?

In this seminar, Investigative Practice examined how the traditional art of cultivating a source works where trust must be won remotely – and whether practices from the digital age can inform traditional methods.

Chair:

Stephen Grey

Reuters

Panellists:

Gabriella Coleman

Anthropologist and author of ***Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous***

Ed Moloney

Irish journalist and writer of ***A Secret History of the IRA***, ***Voices From the Grave and Paisley – From Demagogue To Democrat?*** *and co-producer of the documentaries* ***Voices from the Grave*** *and* ***I Dolores***

> "There is a risk that when you work in one area for a long time that you can be accused of being an informant."
>
> Gabriella Coleman

Online sources

Gabriella Coleman was certainly accused of being an FBI informant during her research work using Internet Relay Chat (IRC), a messaging method used by Anonymous activists among others. It's also worth remembering though, that when working with sources and especially in the areas of computer hacking or national security, it's likely that some of the people you are talking to are informants themselves. Before Sabu was revealed to be an informant, he sought out Coleman and was fishing for information on other sources.

Though she didn't know that he was an informant, she was well aware of the possibility that he, like any of her contacts, could be. It's important to silo information between people, to keep information on different sources separate and ultimately protect those you are working with.

Sources often have their own agendas, which is an issue that journalists have to be aware of and navigate. Journalists have to be careful what emails or information they accept online. Coleman was offered the Stratfor emails in 2011 after they had been acquired by Anonymous activists but she didn't accept them. They were then published as the Global Intelligence files by Wikileaks in 2012.

Coleman has written about the lessons around cultivating online sources that can be learned from the ways in which journalists interacted with and reported on Anonymous in its early days. There are some key points to remember:

Get stories right and put in the time to learn both technology and cultural norms

The hackers at Anonymous felt misunderstood by a lot of the mainstream press. Online sources are generally very aware and potentially critical of different journalists and their work. They will often choose which journalists to go to so it's important to get stories right and behave ethically.

Treat sources and subjects ethically

The journalists who were the most successful with Anonymous were those who dedicated time and effort and were willing to learn: both the cultural norms and the tools, such as IRC.
Remember that sources are people!

Ensure you know (and are seen to know) how to use encryption technology responsibly

Digital communications can be risky but when used well can be secure. Through these means, hackers can get information to journalists safely, but journalists need to protect themselves as well.

Online Sources *Continued*

It's easy to get a false sense of security when using secure communication methods, such as encryption. Journalists should trust encryption as a tool, but not their own implementation of it. But security is a process, not an outcome. Digital security knowledge needs to be constantly refreshed because it is constantly changing. But never over-trust the tools and don't ever get cocky about your security set-up.

A hybrid of offline and online communication is a good model – balancing security and convenience. It's important to compartmentalise communications with different sources because otherwise if one source's identity is revealed, then others are also put at risk.

Sometimes digital contact is inevitable and journalists must also consider their sources' implementation of the tools to secure this contact. The people within Anonymous whose identities were revealed made mistakes themselves, and sources can sometimes compromise themselves even through the initial contact, such as emailing a journalist from a work account. If you are worried that a potential source has already compromised themselves in contacting you, the best way to deal with it is to ignore certain requests until you can communicate with that source in a more secure way. There are also certain countermeasures that can be taken against surveillance of communications with sources, such as obfuscation. For example, if your phone records are available to authorities, it can help to make a lot of phone calls in order to make metadata more difficult to analyse.

Benefits and opportunities of online sources

While there are many reasons to be careful of digital communication with sources, it's important to remember that digital communication tools do present opportunities that didn't exist in the pre-digital age.

Case study: Citizen's Commission to Expose the FBI

Seven activists who broke into an FBI office and took away many files and passed some to journalists. The COINTELPRO scandal followed from this as those journalists used FOI to obtain further information. Those activists were never charged, they were only identified once the statute of limitations had expired, but they did take enormous risks to get those files out and into the hands of journalists.

There are now much less physically risky ways to obtain these kinds of documents. But the question of what you can do for protection is still very important.

When talking to anonymous sources online, documents become even more important because it's harder to verify who the person is and what they are telling you.

Offline sources

During the Troubles, any sort of communication that wasn't face to face was a huge risk. Even a phone call could be risky, because there was surveillance being carried out by both of the British intelligence agencies as well as the IRA. You had to assume that phones had been tapped and someone was listening.

The stakes were so high that it took a long time to build trust with sources. It took old-fashioned methods of lots of face-to-face meetings and lots of patience.

Ed Moloney had to break a big story to demonstrate to other sources that he was trustworthy. He had spoken to the supplier of weapons that killed the lawyer Pat Finucane. He only published nine years later when his source was arrested and charged. Scotland Yard demanded Moloney's material, but he resisted. This showed he was willing to fight to protect his sources and that went a long way towards winning him the trust of others who then became willing to speak.

> "In Northern Ireland during the Troubles, the idea of contacting a source over the internet would be sheer madness."
>
> Ed Moloney

Journalists need to be similarly careful with any sort of digital communications, especially in dangerous countries such as Iraq or Mexico. In these sorts of places, it is also a good idea to use taxis rather than a personal vehicle.

Meeting a source in person is also useful for putting a face to a name and working out whether they are trustworthy. It is always a two-way relationship, so it's actually just as important a process for the source to work out if they trust the journalist. Every source is different though, so it's necessary to meet them and gradually build up an instinct for what works and what doesn't. However, this doesn't necessarily mean face-to-face meetings. Chatting to someone online a lot can in some cases serve the same purpose.

In the same way as you can build trust with online sources by building an intimate knowledge of a subject or subculture, writing about a subject for a long time is also a good way to cultivate in-person sources – because, provided you write about the subject ethically and accurately, they will start to come to you.

Where do we draw the lines?

The New York Times has a policy that sources shouldn't be friends, but in many cases that can be impossible. Having a close relationship with long-term sources can also help you understand their motivations and possible agendas.

However, there are some potentially difficult dilemmas involved in these relationships. It may well be crossing a line to warn a criminal source of a police investigation or teaching them techniques to hide their online presence or communications if they are using these techniques for criminal acts. Moloney, though, would argue that if a source's physical safety is in danger then a journalist has a moral duty to warn them if possible.

Journalists also have a responsibility to think about whether it's in a source's best interest to disclose sensitive information. "Do you really want to tell me this?" It can be surprising how ready some people are to trust journalists, even when told that the journalists cannot control the headline or who will read the information they pass over.

If you pay a source for information though, that information is tainted.

10 tips for source cultivation, Stephen Grey

1. "Dress like them" – make sources feel comfortable by entering their world, respecting their values and acting like them.
2. Protect them and yourself.
3. Use gatekeepers – the best sources introduce you to others and can vouch that you're trustworthy.
4. Make a legend – your reputation is crucial so be known, prove yourself, become an expert.
5. Shun motives – you can't get into the mind of every source. Verify what you can but there is a limit to what is possible.
6. Avoid making people lie – don't push sources on topics they aren't happy to talk about. Once they have lied to you once, it becomes a lot easier.
7. Take time – don't look rushed, lean and hungry, because people won't trust you. Invest your time and show willing.
8. Make friends – get to know your sources so you share common experiences.
9. Work isn't everything – entertain people, get to know them. Professional relationships bring less reliable information because sources want something, but if they know you they are more likely to give you information without wanting something in return.
10. Show something of yourself – gossip, give a little to get something back.

10 tips for source cultivation, Stephen Grey *Continued*

Some additions were suggested:

- Get to know anthropologists in your area and earn their trust as they will have a good grasp of the issues and can make the best gatekeepers.
- Cultivate a strong liver first...

3

Blowback: The Dangers of Whistleblowing – For Both Sources and Journalists

Gill Phillips
Phil Chamberlain
Bill Goodwin
Julie Posetti

Proceedings of seminars at
the third international
CIJ Logan Symposium

London, 19/20 October 2018

Goldsmiths, University of
London

Blowback: The Dangers of Whistleblowing – For Both Sources and Journalists

The need for stronger protection for whistleblowers is regularly discussed but far less attention is given to addressing the dangers of whistleblowing before the decision to raise concerns has even been made. How can we help those who want to speak up about corruption or abuse to do it in ways that minimise these dangers before it's too late? And ways that maximise the chances of getting a good outcome for both journalist and source?

In this seminar, Investigative Practice aimed to move beyond general calls for whistleblower protection after the fact to identify more effective and safer methods for divulging information in the public interest.

Chair:

Gill Phillips

Director of Editorial Legal Services, The Guardian

Panellists:

Phil Chamberlain

Journalist, academic and author of ***Blacklisted***

Bill Goodwin

Investigations Editor, Computer Weekly

Julie Posetti

Senior Research Fellow, Reuters Institute for the Study of Journalism, Oxford

> "We've seen overreach of national security and anti-terrorism law in combination with the surveillance state, bringing disruption to the practice of investigative journalism and enormous risks to journalists and their sources."
>
> Julie Posetti

While working on the UNESCO report 'Protecting Journalism Sources in the Digital Age', Julie Posetti has documented an increase in the undermining of source protection legislation and structures in the UK, US, EU, Australia and elsewhere. This threatens not only the confidentiality of journalist-source relations, but also leaves journalists and sources prone to criminal sanctions and imprisonment; financial sanctions such as loss of income, employment and opportunities; and in certain situations where journalists are reporting on national security agents or conflicts, the risk of kidnap, torture or targeted murder. This obviously produces a chilling effect that deters journalists from working on sensitive stories and sources from speaking to journalists in the first place.

Though there is a level of legal protection for sources in most jurisdictions, in practical terms there will still be a lot of pain for both journos and sources. There's a pressing need for both to be tech savvy before the fact, which is the Catch 22 in this situation.

> "Whistleblowers tend to come to reporters at the end of a long, stressful and damaging internal process."
>
> Phil Chamberlain

Blowback and risk can be interpreted slightly differently, for instance the example of Phil Saviano. There's a scene in the film *Spotlight* in which Saviano arrives at the *Boston Globe* offices with boxes of source material and is asked why he hadn't come in before. Saviano has to explain that he had approached the newspaper previously but wasn't believed in large part because of his vulnerability.

Are we equipped to deal with people who have been damaged by their experiences in this way as journalists? Traditionally, journalists tend to approach a source quite coldly. Are we equipped to take on a duty of care, especially with mentally vulnerable and damaged whistleblowers.

The NHS seems to be especially bad in terms of how they treat those who raise issues internally. Often the reporter is the last person a whistleblower will come to, so there's a need for journalists to prepare for this kind of 'pastoral care' as well as digital security care. But there's also a duty of care to yourself as a journalist due to the kind of stress that comes from taking on this role.

Several questions arise around morality in these relationships:

- How far does the motive and background of the source matter?
- What ethical responsibilities does the journalist have for the source?
- Where does that ethical responsibility end?

There will always come a time when a journalist will need to find the point in which to step away from this relationship and say 'I need to write what I need to write' whether or not that's what the source wants to tell you.

> "If you blow the whistle it's a life-changing decision, which is why Public Concern At Work's advice is generally 'don't blow the whistle'."
>
> Bill Goodwin

Whistleblowers are different from confidential sources. They are often very traumatised people and see things through a traumatised lens, even when they appear to be very together. It can often be like being a counsellor, the main need of many whistleblowers is for someone to listen to them and journalists often end up taking on this pastoral role in which there are dangers from both taking on stress and getting too close to a story. The key thing for the journalist is to get hold of the documentary evidence, but they should bear in mind that there's almost always a difference between what the whistleblower sees through their traumatised perspective and what's in the documents.

The surveillance of whistleblowers and journalists is also very worrying. There have been several reports proving that the security services and police are targeting both for surveillance, including the 2015 report from the Interception of Communications Commissioner which revealed that police forces have used the RIPA legislation to spy on 82 journalists and 200 sources suspected of being in contact with the media.

Some good advice was given to Bill Goodwin at the first LOGAN Symposium by the New Zealand investigative journalist Nicky Hager: "If you're meeting a source, you don't ring them, you don't text them and you don't take your phone with you, that's pretty simple. If you contact your source by phone you're a bloody idiot these days."

This is not just good advice when meeting a source, but it can apply to meeting your legal editor too. In Gill Phillips' experience, for instance, similar measures were required when she met Ewen MacAskill in Hong Kong and was briefed on the Snowden case in a concrete park without any kind of electronic devices with them. These are basic journalistic toolcraft, but the pace of recent technological change in society has produced new context which takes some adjusting to.

Most concerning from a legal point of view is that with the passing of the Investigatory Powers Act, the state no longer needs to request source material from journalists, they can go straight to a telecommunications provider and request details of communications without the journalist or newspaper ever having any knowledge of either the request or the release of information. Under the previous legislation, PACE, while not a perfect situation, journalists and publishers at least knew what was being requested and were afforded the opportunity to make a case in court for refusal.

The Signals Network is a foundation which provides resources and support for both sides of this equation, helping media to work better with whistleblowers in France, UK, US, Germany and Spain. They provide their media partners with contacts of lawyers who work pro bono to advise whistleblowers pre-publication and can pay legal fees post-publication.

This can help in situations where paying for legal advice for whistleblowers can present a conflict of interest for a media organisation or where the legal team of a publisher is not in a position to provide independent advice to the whistleblower. It's important, for both sides, to remember that the journalist's interests are not always the same as the whistleblower, even though sources will often look to the journalist as their protector. Journalists need to be very wary about putting themselves too much in that position.

From the perspective of a media legal team, it can be difficult to strike a balance between directing a whistleblower to a place that can provide practical independent advice, while ensuring that they're not dissuaded from blowing the whistle entirely. There's not many places which can provide advice that strikes that balance and The Signals Network is trying to address that shortfall.

With regards to the motives of whistleblowers, Marty Baron of *The Washington Post* argues that it's the duty of the journalist to look at the public interest in the information being provided, while it's the work of civil society and the editorial page to examine the motives.

Q

What should be the priority of concern between the risks of prosecution from the state, or physical harm from organised crime?

A

From Posetti's experience within the Australian context, organised crime is becoming more and more problematic. While there's a lot of awareness about the need to mitigate the threat of digital surveillance to sources and whistleblowers when working on national security-oriented stories, this is less well recognised when investigating organised crime. The technology and techniques available for digital surveillance are becoming cheaper, more user friendly and increasingly ubiquitous. Due to this, the threat to confidentiality of communications within organised crime reporting has become just as important to be aware of and develop countermeasures to as it is on the national security beat.

It depends to some extent on the national context, the political context and the nature of the story. However, one of the points that underpinned Posetti's work was that reporters cannot reasonably argue that they're just a sports reporter so have no need to increase their level of digital security because if they're reporting on international football, or the Olympics, then there are real and credible digital surveillance risks that stem from links between those industries and organised crime. The same can be said of the fashion industry; organised crime connections exist with some of the international fashion houses as well as in the clothing manufacturing industry.

This territory constantly intersects so there is a need for every journalist, no matter what beat or patch they work on, to increase their base level of information security to get as clean as it practically can be. It is possible (though not necessarily advisable) to reduce your level of digital security while working on an investigation, but it is often almost impossible to effectively increase it after your work has begun.

Border crossing is a particular risk. Mohammed Rabbani spoke at the Symposium about his involvement in a situation in which Schedule 7 anti-terror legislation was used against him to attempt to force him to provide the passwords to his devices to law enforcement. There is a provision in the Regulation of Investigatory Powers Act that makes withholding a password in such a situation a 'strict liability offence' meaning it is an immediate criminal offence which carries a potential prison sentence.

The other problem with source protection in the technological age is that the authorities view a computer or a phone as one item, so all information can and will be collected from them. In the pre-digital context, authorities raiding a journalist's office could be told that certain files contain journalistic material and would therefore be required to place that into what was colloquially called a 'blue bag' which would then be sealed. That seal could not be broken unless there was an independent lawyer present to go through the material and assess it.

That's no longer possible when all kinds of information is stored on a single device and a journalist can't argue that certain elements of the stored data are journalistic and therefore should require independent assessment. The only way today's journalists can guard against this is by taking precautions before they find themselves in a situation where they're faced with this problem.

Remote collaboration between journalists and whistleblowers across borders is another area where these issues can cause problems. There are secure tools available but journalists should take notice of which national jurisdictions the servers for such tools are based in, and check what restrictions or obligations there are on companies in those jurisdictions to hand over or allow access to servers to government authorities and security services.

There is an encroaching sense of danger to journalists from both the state and organised crime, particularly with the murder of Daphne Caruana Galizia in Malta a year ago, of Ján Kuciak in Slovakia in February and the recent murder of Viktoria Marinova in Bulgaria.

In the UK, the state is far more likely to attempt to crush the source rather than target the journalist. There are at least some protections for reporters here, but the state cannot allow it to be seen in any sense as easy to pass information to journalists. This is complicated by both the bleedover from other areas into organised crime, but also by the change in definition of what a reporter is, especially in the current context where so many are working as freelancers or in other contexts where they won't necessarily have the protections afforded to them by the organisation that is publishing their work. That's why some of the organisations represented at this Symposium who are working to address that lack of protection are so important, but in this context where the source will be the target, the protection of that source is absolutely fundamental.

Relevant legal cases

Goodwin was the subject of long-standing jurisprudence around source protection in the European Court of Human Rights case, Goodwin Vs the UK.

A little over three months into Goodwin's first job as a journalist, he was contacted by a confidential source with information about the financial difficulties at a software company called Tetra Business Systems. Upon contacting the company for comment, Goodwin received a fax outlining a superinjunction against publication of the story, but also any mention of the injunction itself. Goodwin was forced to break the law in telling the NUJ about the situation and became the subject of civil litigation, the hearings for which took place *in camera*, excluding both the press and public.

Relevant Legal Cases *Continued*

During the court of appeal hearing Lord Donaldson requested that Goodwin put his notebook in a sealed bag, which would be opened if the appeal was lost, thus revealing the identity of the source and there were threats to obtain a search order for Goodwin's flat. He enlisted the help of a friend who visited the flat and took everything that could be compromising for source protection to an undisclosed location, known to no-one else, including Goodwin.

The case eventually reached the ECHR, where the company had a right to send Goodwin to jail. In the end they declined to, ostensibly as 'a gesture of humanity', but in reality to avoid the negative publicity that would come from the company being named.

The other relevant ECHR case involving UK media is Interbrew SA Vs. Financial Times Ltd. and Others, which highlighted the pressure that this puts on the relationship between journalist and the organisation as there was a threat that the court would impose a £5,000 rolling fine for each day that a document that had been passed to journalists was not turned over. The lesson of this is the need to separate out responsibilities; with the journalist taking responsibility for the protection of the source's identity, so that the organisation can legitimately deny knowledge of that identity. If the editor knows, then the organisation knows and this can make the situation more difficult. Even more important is not to disclose the identity or pass source material to an organisation's legal team, as lawyers are bound by duties to the court that do not apply to journalists.

There is also a need to be aware of the risk of making a moral judgement to release notes, documents or the identities of sources in certain cases but not others. If a journalist releases such information in a case where they feel it is morally right to do so, this can leave them in a much more difficult position in future cases where the moral judgement seems less clear cut.

There are also questions around where lines need to be drawn. Many journalists would see it as acceptable to buy a drink for a whistleblower, or buy them dinner, put them up in a hotel or even buy a burner phone, but as you go further in this escalation you start to push against the boundaries of acceptability and put yourself of legal risk in terms of incentivising a source to provide a story. Phillips was involved in a case where the journalist had bought a burner phone for a source and the state argued that constituted bribery. In the end, it was proved that the purchase happened a considerable time after the contact between them began so the charge was undermined, but the case highlights how careful journalists need to be with their relationships with sources.

Q

What measures can be taken to mitigate the risk of being prosecuted for refusing to disclose a password or decrypt files?

A

There are some simple measures, such as splitting a password or asking someone else to set a new password when you are at particular risk (for instance, when crossing borders) so that you know only half of or only an old password and are literally unable to decrypt files when requested to.

There are also technological measures that can be taken, for instance setting up an encrypted file with ostensibly sensitive documents within, as well as a hidden encrypted drive in which to place the documents you are really worried about others accessing. In that case, you can then comply by revealing the password of the first encrypted drive, without compromising the actual confidential information you are storing or carrying. The TAILS system has a function dedicated to this purpose.

Q

What resources and support are available for freelancers on these issues?

A

The Journalists in Distress Network is a group of 18 international organisations who provide journalists with resources, help and referral services on both legal and technical issues regarding source protection. The Committee to Protect Journalists lists the organisations and how they can help.

Legal support

The National Union of Journalists can provide members with advice and representation on issues such as protection of sources, production order applications and seizure of materials/equipment and restricted reporting orders.

The Media Legal Defence Initiative can provide training, advice, representation and in some cases funding to help with legal costs to journalists bloggers and independent media outlets around the world. They also run Media Legal Defence Centres in several countries.

The Signals Network is a foundation which provides resources and support for both sides of this equation, helping media to work better with whistleblowers in France, UK, US, Germany and Spain.

Technical support

The Centre for Investigative Journalism can provide one-to-one guidance for journalists in securing their data and communications and run a drop-in information security clinic for all delegates at their Summer Conference and the Logan Symposia. They have also published several video tutorials on using encryption and information security tools.

The CryptoParty movement is a decentralised, global initiative organising free and open events where digital privacy rights are discussed and open-source anti-surveillance tools are taught.

The Freedom of the Press Foundation offer guides and training in digital security. They also support Signal, the end-to-end encrypted private messaging app, and SecureDrop, the anonymous secure whistleblowing system.

The Electronic Frontier Foundation run the project Surveillance Self-Defense providing tips, tools and how-tos for secure communications and data.

The Tactical Technology Collective provide several toolkits and guides, including the Security in a Box project.

Whistleblowers and sources: some useful references and resources

Compiled by Gill Phillips

International Standards

- Universal Declaration of Human Rights (UDHR) 1948
- Articles 8 / 10 of the European Convention on Human Rights 1950/1953
- Articles 17/19 International Covenant on Civil and Political Rights (ICCPR) 1966/1976
- Inter-American Human Rights System
- African Human Rights System
- League of Arab States
- Association of Southeast Asian Nations

European standards

- Committee of Ministers Recommendation No. R (2000) 7 on the right of journalists not to disclose their sources of information
- CoE Parliamentary Assembly Recommendation 1950, Final version, The Protection of Journalists' Sources, 2011
- CoE Parliamentary Assembly Resolution 1729 (2010) and Recommendation 1916 (2010) "Protection of "whistle-blowers"
- Committee of Ministers' Recommendation CM/Rec (2014)7 to member States on the protection of whistleblowers adopted on 30 April 2014
- Committee of Ministers' Recommendation CM/Rec (2016)4 to member States on the protection of journalism and safety of journalists and other media actors
- Declaration of the Committee of Ministers on the protection of journalism and safety of journalists and other media actors (Adopted on 30 April 2014)
- CoE Parliamentary Assembly Resolution 2045 (2015) on Mass Surveillance

Whistleblowers and sources: some useful references and resources

Compiled by Gill Phillips
Continued

Reports

- 2015 Report of the UN Special Rapporteur on Protection of Sources and Whistleblowers
- Feb 2017 : Dr Judith Townend and Dr Richard Danbury IALS Report : 'Protecting Sources and Whistleblowers in the Digital Age'
- Julie Posetti : UNESCO - Protecting Journalism Sources in the Digital Age

Resources

- Columbia University – Global Freedom of Expression: Law Standards

  Cases
- Reporter's Committee Compendium Guide on Reporter's Privilege in the US
- Council of Europe Factsheet on Whistleblowers and their freedom to impart Information
- European Court of Human Rights Factsheet on Protection of journalistic sources
- Carlo, S. & Kamphuis, A. (2016) Information Security for Journalists, Version 1.3, The Centre for Investigative Journalism
- Endert, J. (2017) Digital security resources, DW Akademie
- OSCE Safety of Journalists Guidebook, 2nd Edition 2014
- Council of Europe Platform to promote protection of journalism and the safety of journalists

4

On the Ground and in the Ether

Chris Woods
Iona Craig
Anand Gopal

Proceedings of seminars at
the third international
CIJ Logan Symposium

London, 19/20 October 2018

Goldsmiths, University of
London

On the Ground and in the Ether

War reporting is changing: reams of data and munitions expertise can now be brought to bear without ever setting foot in a war zone, while the access of officially 'embedded' reporters is heavily subscribed, leaving it to freelancers to take the huge risks necessary to get the story out. Analysis of data and social media opens up unprecedented new opportunities for warzone reporting, but does it also open journalists up to manipulation?

In this seminar, Investigative Practice asked how online research and on-the-ground reporting can most fruitfully work together.

Chair:

Chris Woods

Founding Director, Airwars

Panellists:

Iona Craig

*Freelance reporter and founder of the **Yemen Data Project***

Anand Gopal

*Journalist and author of **No Good Men Among the Living: America, the Taliban and the War Through Afghan Eyes.***

> "The role of the field correspondent is crucial in not just telling stories but also framing our understanding of civilian harm."
>
> Chris Woods

The need for on-the-ground reporting

On-the-ground reporting is in decline. This is a fact made evident by an Airwars report, examining the media's coverage of civilian casualties in Iraq. What they found was that during the first two years of the war against ISIS in Iraq, not a single report from a mainstream media outlet was carried out from the ground. The reason why this is so problematic is because the Pentagon uses mainstream media field coverage as a metric in determining the extent of civilian harm.

This gulf then has to be filled by people from those countries. For instance, Iraqi and Syrian civilians self-reported, predominantly through social media, more than 26,000 casualties from Coalition actions since 2014. A similar number of civilian fatalities have been reported in the same way from Russian actions in Syria alone. Why aren't we listening to those voices?

So in this world where our governments fight remote wars, given the general absence of reporters on the ground but with so much information online how do we ensure that the effects of those wars are properly understood? And what are the risks of these new methods?

> "It's about having a specialism."
>
> Iona Craig

Iona Craig has been reporting from on the ground in Yemen for several years, and also working with the Yemen Data Project so her work spans both the methodologies in question.

Reporting using data

In using data to form stories, anonymity is often crucial. This is something Craig found key when working with the Yemen Data Project. A lot of their data was open-source, taken from Whatsapp groups, Youtube and Twitter but also from local media and local activists. A difficulty they found in establishing the project was gaining the trust of international media and journalists. Some were concerned that the data was being used to push a political agenda: 'a front for the Saudis or the Houthis.' Their way around this was to be as transparent as possible about their methodology and its possible flaws.

More generally, the demand to report on her findings as a journalist was sensitive to changes in global politics. For instance, Craig pitched a story about disappearances in Yemen to five different publications around the time of Trump's

Reporting using data
Continued

election, and had no uptake. Another problem in spreading these stories is that there seems to be an audience bias towards foreign correspondents, having a foreign correspondent going in is somehow seen as more legitimate than a local voice telling that story. For example, when writing a piece about the navy SEAL raid on Yakla in 2017, Craig found that her article had a lot of traction in spite of its slow release and the fact the Bureau of Investigative Journalism had already covered the story with a Yemeni reporter. This seems to be a cultural issue within the media industry and in the media consumption of the wider Western public.

Reporting from the ground

The obvious advantage of reporting from the field is that you gain first-hand experience of the territory you are reporting on, importantly of local dynamics, politics and internal biases. Craig found that building relationships with locals and having local knowledge gave her special access to stories she wouldn't have had otherwise. When the Saudi Coalition air-campaign began, she was able to get into Yemen by boat when many other journalists were refused. Having spent a lot of time there, she was given permission from tribal leaders to go to certain places because they had a clearer understanding of her intent and trusted her.

The other advantage her time spent and connections in Yemen afforded her was the knowledge of local power structures and different political factions. This allowed her to unpick the different biases and contradictory claims that are evident in reports coming out of the country in a way that others without that local experience and knowledge would not be able to. Having put in this time and work to understand the place and the people living there provides advantages in reporting both on the ground and remotely using data and open-source evidence.

> "In pursuing ground-based stories, there are a variety of obstacles to navigate."
>
> Anand Gopal

Reporting from the ground
Continued

Funding:

It is difficult to get stories funded that involve going into the field. Anand Gopal's project, The Uncounted, on US-led coalition actions in Iraq was rejected by multiple outlets before it was taken up, for instance. His project visited 103 sites over the course of three years, demanding a lot of resources.

Lack of infrastructure:

Gopal found that in Iraq, unlike in Syria, there was no active local media network. This meant that events were not being reported online, making ground investigation even more crucial.

Complexity of fighting:

On the ground, it is difficult to decipher responsibility for civilian harm especially in conflicts with many different actors such as the war against ISIS in Iraq. Gopal got round this by visiting every single impact site to determine what munitions and artillery type were used for each strike and who was responsible.

Incomplete records:

Gopal's method was to send the coordinates of the strike sites to the Coalition to ask solely if they bombed that location. The majority of those strikes did not involve civilian harm; they were either empty structures or ISIS targets. So by asking simply whether a given location was targeted, and not addressing the reasons for targeting or the nature of what they were trying to hit, they were able to access a different response mechanism from the Coalition bureaucracy which then gave them yes or no answers for each of the sites that they had studied. Unfortunately, the records those answers were based on turned out to be inaccurate or incomplete, as demonstrated by the Coalition claims that they had not struck a location for which they themselves had uploaded video evidence of striking.

Bureaucracy:

Getting answers, even inaccurate ones, as to why a region was targeted, is an even more difficult process. A common route is to make an FOI request but the issue here is that they can take an extremely long time to process. The way they circumvented this is by stressing the danger that some of the victims were in. For example, in the case of Basim Razzo, one of the survivors of an airstrike reported on in The Uncounted, the Coalition records and the footage of the airstrike they published stated that Razzo's home was an ISIS IED (Improvised Explosive Device) factory, and the deaths of his wife and children were allocated to a column recording the deaths of ISIS fighters.This left Razzo at huge risk of being further targeted by the Iraqi authorities for his alleged ISIS sympathies.

Reporting from the ground *Continued*

This approach did work in terms of getting answers from the Coalition bureaucracy much more quickly, within two or three months, but a further issue is that these loop-holes close up when they are used too often, which meant the government stopped fast-tracking Gopal's FOI requests, despite there being hundreds of other civilians in similarly dangerous situations. He then resorted to suing the US government to speed up the process.

Q

Is there a bias towards stories from foreign correspondents over those from local journalists with all international journalists or just those based in Western countries?

A

What seems to make the difference is if the story is covered by an American mainstream media outlet, specifically. For instance, if you look at Colonel Ryan, the spokesperson for the Coalition, all the outlets and journalists he follows on Twitter are American. In this sense, it is not so much about getting a journalist from a western country, as it is about getting the backing of a US outlet.

It is important that when you are pitching a story to a US outlet, you get some interest even if not a direct commission prior to your trip because they will want an editorial input throughout the investigation: which characters to focus on or what angle you will take, for example. It is also good to have some kind of institutional support whilst you are on the ground, even when you are freelancing, though this may of course be easier said than done. There is also the issue that you cannot ever be certain, especially in conflict reporting, whether there will be a story there when you arrive or what form such a story will take, which makes this process of getting institutional support prior to the trip that much more difficult. This is less of an issue with TV, since there are greater resources available and you can often get 'project development' to cover such exploratory work, but when working in print that funding is almost never available.

Q

How do we effectively report on stories that are so fast moving?

A

In the case of the US, they are dropping bombs faster than they can build them, allegedly one every twelve minutes. When the numbers are so staggering it can be difficult to keep monitoring each airstrike.

In the case of Raqqa, which the UN has described as the most destroyed city in Syria, 20,000 munitions were dropped by the Coalition forces alone on the city in less than five months. There was very little coverage of this, though Quentin Sommerville of the BBC and Amnesty have been doing good work trying to understand the events after the fact.

How do we effectively report on stories that are so fast moving?
Continued

But what can be done, as Airwars, Iraq Body Count and others have shown, is to monitor civilian harm from the perspective of civilians, recording claims of civilian casualty events, run rudimentary assessments and then leverage this information for change. The challenge is in getting governments to engage with that information, in order to introduce at least some accountability into the process.

The US military have actually proved reasonably responsive to such pressure and have improved their methods for reporting civilian harm, whereas in the UK the government does not want to concede any civilian deaths at all. The UK is currently involved in wars in Iraq, Syria, Afghanistan and Libya and have admitted two civilian casualty events in the past decade, one in 2008 and one in 2018. These are systemic and cultural challenges which we have to contend with.

To some degree, in counting bombs dropped, you will have to round-up or alter the metric by which you classify an attack. For example, in the case of the Yemen Data Project, they will characterise several strikes on the same target as a single air-raid if it happened over a short time. In terms of air raids, after three and a half years, the records are nearing 19,000 air raids, but in terms of the individual bombs being dropped, it's just not feasible to count.

Q

How can you verify your sources if you are not on the ground?

A

Part of it is intuitive and self-evident, such as in the case of Airwars investigating civilian harm in Syria. They found that the nature of underrepresented stories is that they lack any kind of wider audience in the international community, which means that the very locally specific communities that are reporting most of these incidents have little incentive or agenda to fabricate posts. Airwars also found that these communities were good at self-regulating. They saw this in how local communities fact-checked both inflammatory ISIS claims and the reports of local outlets, through the comments section.

In certain areas such as Yemen it is very difficult to have any system of validation because there is no online community surrounding them to report what is going on. In this situation, you have to rely on word of mouth and pool from your existing contacts. Alternatively, you may have to just visit the location yourself. Craig reiterated that this is a scenario where it is really important to have a speciality because you will avoid the obvious pitfalls of disinformation. This proved essential in questioning the Houthis' inflated reports of civilian casualties or deciphering media biases when you have media organisations with the same name, but directly opposing biases.

Q

How do we validate and verify reports from smaller humanitarian agencies and charities when people are reluctant to trust them?

A

You may be able to assess reports from smaller organisations through speaking to larger sponsors or UN agencies that are working with those organisations on the ground and will have a more informed understanding of the agenda or trustworthiness of each agency.

The other method is to validate content coming from small agencies by cross-referencing against other reports online and using standard verification methods such as geolocation. Ultimately, understanding the credibility of those agencies may come down to a mix of intuition, local knowledge and the experiences of other journalists working in the area.

Bringing the methodologies together

Ultimately what is probably required in complex conflict reporting is a hybrid of both on-the-ground reporting and remote data analysis. In bolstering the credibility of the story, it seems that drawing on both data and on-the-ground reports is the best way forward. It is possible that someone on the ground may exaggerate their experience but it is also possible that official statistics can be inaccurate. As such, it is best to use them in tandem to get a clearer picture of events.

The question really is where the ideal balance, or the merge point exists between these two approaches. In marrying the two, it may call for journalists to elevate and refine new skills, as well as an increase in cross-disciplinary collaborations, especially between the methods and practices of both journalism and social science.

5

Forensic Journalism

James Harkin
Eyal Weizman
Samaneh Moafi
Eliot Higgins

Proceedings of seminars at
the third international
CIJ Logan Symposium

London, 19/20 October 2018

Goldsmiths, University of
London

Forensic Journalism

From open-source digital mapping to forensic architectural methods to the kind of data journalism which can aggregate and divine patterns in the ether, what might be called forensic journalism – the application of methods drawn from science, technology, new media and professional expertise – is rapidly gaining ground.

In this seminar, Investigative Practice discussed the issues which arise for investigation when gifted open-source "citizen journalists" work with professionals, and when both work with traditional newsrooms and NGOs.

Chair:

James Harkin
Director, The Centre for Investigative Journalism

Panellists:

Eyal Weizman
Founding Director, Forensic Architecture

Samaneh Moafi
Research Fellow, Forensic Architecture

Eliot Higgins
Founder of Bellingcat

> "The first big open-source story was probably the Boston Marathon bombing, but for all the wrong reasons, because of the Reddit community's investigation that identified the wrong people and basically led to innocent people being harassed."
>
> Eliot Higgins

The developmental stages of open source investigation

Investigation techniques using open-source information have developed over the last decade or so in roughly 4 stages:

2007–2011

The rise of smartphone use and social media apps lead to huge wealth of reference material becoming available. After the Boston Marathon case, there was a clear need for verification tools and techniques to be developed.

2011–2013

Arab Spring begins and there was lots of social media being shared from that and questions arose as to what was authentic and what wasn't. It also saw the rise of fake bloggers, for example 'Gay Girl in Damascus' who turned out to be an American man in Edinburgh, certainly not in Damascus. Eliot Higgins started the Brown Moses blog, doing basic munitions identification in the Syrian conflict using open sources. At the same time a community was starting to build around the practice, including organisations like Storyful who'd already been working in the field for some years and others interested in arms control. The biggest story for Higgins personally came from using rebel Youtube videos to prove that weapons were being smuggled into the area by Saudi Arabia. Because of the limited access on the ground for journalists, these methods became increasingly important.

2014–2016

Governments started making statements that could be checked against open source information, and criminal investigations, for example the Joint Investigation Team, began used open source material. Also growing interest in the practice from many different bodies.

2017…

We are now seeing large international bodies like the International Criminal Court (ICC) and the International Impartial and Independent Mechanism (IIIM) which was set up by the UN General Assembly to gather evidence and build cases around international crimes in the Syrian conflict. These bodies are now taking open source investigation extremely seriously in their work. In August 2017, the ICC issued an arrest warrant for a commander in Libya based on Facebook videos.

In terms of how the process has developed, there's a much wider network now and much more collaboration between those recording the material on the ground and those analysing it, so there have been initiatives to train activists in how to collect such evidence in ways that will be more useful to analysts.

Open-source archiving

The main challenge the practice is currently facing is mostly one of data management. How do you archive huge amounts of material such as the 1 million videos collated by the Syrian Archive in ways that are searchable and accessible, but that are also still forensically sound and can regulate who has access to the material? The other question is how to ensure it's preserved, not just for five years, but for 25, 30 or 50 years? These are the questions that the ICC and the IIIM, helped by a wide coalition of organisations, are now really focused on finding solutions to.

There's obviously a great need to enable this kind of archive building work, but there are also several potential problems around it, from witness protection issues to organisations that are reliant on the collection and collation of this source material for their funding so are unable to provide it to anyone for free. Then there are problems with practicality, especially when you get to the point of having 20 or more separate archives.

Bellingcat are working with the Syrian Archive and others to build the Archive for Conflict Investigation, a searchable system in which hundreds of thousands of pieces of source material can be indexed using unique identifiers but without making copies of the material itself. It will allow organisations to choose how much detail on their material they wish to share, from just date/time and geolocation data up to much more detailed information, and then other organisations such as the ICC can search the index and send out automated requests for the actual material that is relevant to their work.

Automated open-source investigation

With the exponential increase in source material we are getting beyond the situation where the work of analysis can be effectively done by a team of dedicated human researchers. There's also a need to develop automation and machine learning for open-source investigation. Forensic Architecture are working on projects to train algorithms to search for and recognise particular munitions or other objects or events of interest to an investigation.

The Syrian Archive are currently developing this capacity for identifying cluster munitions and they have a huge amount of source material with which to train such an algorithm. It's important for these future systems to be modular, so that multiple organisations with different budgetary constraints can all get practical use out of them, while at the same time ensuring the creation of a community that allows people to help each other and supports and advances the work of multiple organisations. Higgins' initial work was of course facilitated by a huge number of free tools and platforms that made it possible so it's important to build this in to further projects as far as possible.

Automated open-source investigation *Continued*

This is absolutely essential for justice and accountability in the future, since Syria is by no means a unique case; Bellingcat are already working with a range of organisations on a similar project focused on the conflict in Yemen.

Examples of use cases:

53rd Air Defense Brigade Investigation

Work on this involved trawling through huge amounts of images from social media, but a lot of that work could easily be automated by, for instance, training an algorithm to recognise uniforms in images or something as simple as identifying every single social media account which mentions the 53rd Air Defense Brigade. You could then use that to automatically map that network and flag up the most interesting and relevant parts of it, or scrape all the images available and dump them into an archive for analysis.

Military movements through the Bosphorus

Bellingcat are looking into using web cameras trained on the Bosphorus, and deploying machine learning taught to recognise vessels in the first place, and then specific military vessels as the algorithm becomes more sophisticated, in order to monitor military movements in the region.

There are ethical issues that are thrown up by automation of this type since it could be used for a range of different purposes, some less ethical than others. Other problems relate to the transparency of the methodology when using automated or algorithmic processes of open-source investigation. One of the important things to do in these investigations is to show the methodology, especially if you're using the process to establish facts or some kind of 'truth'. So there is a challenge to ensure that where AI is used for this, we find ways of ensuring that the explanation of the methodology is still communicated clearly and in an accessible way.

> "What we do insist on when we publish with organisations like the New York Times, is to have our own story."
>
> Eyal Weizman

Automated open-source investigation *Continued*

Precise architectural spatial models are a way of creating relations between images that are otherwise very hard for people to see the relations between. It's about navigational viewing, you have a model in which you locate dozens, hundreds or sometimes more sources in space and time and the model becomes a way of navigating between sources. This can include image sources, audio and video sources, sometimes material evidence that is found on the ground of a particular incident.

In terms of the history of the practice, Eyal Weizman's work prior to Forensic Architecture was looking at war crimes committed by architects by examining the way Israeli architects were using their own tools of the trade to design settlements, borders, fences, checkpoints and other pieces of infrastructure in the West Bank in order to effectively squeeze people out as part of a policy of ethnic cleansing. Following that he began an alternative practice of contemporary archaeology, analysing the ruins of buildings to determine facts about the course of events.

> "We can understand the link between certain things and how events have unfolded, but also pinpoint areas that were blind spots."
>
> Samaneh Moafi

So Forensic Architecture like to work with other organisations but often have a slightly different emphasis and always reserve the right to publish separately. In the Douma case, for instance, they published something significantly separately from The New York Times, their media partner.

There are other ways in which these techniques can be used, beyond what is normally thought of as 'open-source investigation'. Forensic Architecture are working with forensic psychologists to develop a practice of 'Situated Testimony' which uses techniques such as 3D modelling and building a representation of an event to bring back certain memories which have eluded a witness or enhance the clarity and remove distortion from existing memories. Sometimes a basic and potentially crude distinction is made between testimony and evidence and this practice provides a way of breaking down this distinction and weaving together both elements in ways that reveal a great deal.

Automated open-source investigation *Continued*

We also need to remember that testimony can be gleaned from recorded footage and imagery. A camera records from both its ends and it's not only what is in the frame. The work of joining together these sources is one of linking all these details and capturing the full story from what is both inside and outside the frame.

Forensic Architecture are working on frameworks which bring together large bodies of evidence into a 3D model to locate them in time and space, but also ensure that the analysis is streamlined so that you can pinpoint events or identify links very quickly and easily.

But the interesting thing is how this process also highlights the gaps in the story and brings into focus the information that we couldn't see or that we don't have access to. And this allows us to identify areas for further investigation.

Q

What sort of verification and fact-checking processes do you use?

A

At Bellingcat there's an awareness that many people are very ready to attack the organisation if they publish something that's not verified or turns out to be incorrect, so the editing process is long and painstaking. Investigators there are constantly critiquing each other's work. There are often long periods where members on a project will debate the precise language used to describe certain objects or ideas.

Working a lot with other organisations, as in the recent Anatomy of a Killing project with the BBC and Amnesty International, means there are many different backgrounds and perspectives being brought in to this process. The best perspectives are often those of the enthusiastic amateurs, as they're not working for any organisation and just want to find out what's true so they will challenge people and put theories to the test. But generally it's possible to have a sensible discussion and come to a conclusion. When Bellingcat and Forensic Architecture collaborated on the M2 Hospital investigation both organisations ran fact-checking processes on the source material to test each other's theories and produce reliable accurate work.

There's a need to distinguish between the top-down hierarchical process of fact-checking, and verification which comes from the collision and entanglement of different expertise and perspectives. Open-source investigation as a practice generally leans more towards the latter - an almost wiki-style process where many people are correcting and checking each other.

Q

Does locating this work in an arts space, as in an exhibition, make the data more difficult to refute by anchoring it in a 3D space?

A

Conversely, in the art world as an institution, fact and fiction are in an unstable relation to each other, so it's not really articulated as a 'truth-producing' institute like a court, scientific lab, university, etc. This makes it difficult to explain to people watching something in an art gallery that what they are seeing should be taken as fact rather than a fictionalisation and this is being used continually against us.

So while it's very important both in producing and funding Forensic Architecture's work and in seeking new audiences for their investigations, they often have to defend themselves for having worked in galleries. In fact, they have lost commissions due to the recent Turner Prize nomination, with people saying that the optics on the organisation is now that they are not serious investigators.

On fact vs. fiction though, having access to gallery space and an arts-based forum allows for a different sensibility in understanding events and incidents. Different kinds of relationships can be brought to the fore, so the understanding can be less about identifying specific people as criminals or events as crimes, but more about understanding systematic crimes that are happening in the contextual space around such events.

Q

How did you find the source material for the Skripal Poisoning Investigation?

A

Bellingcat managed this partly by having people on the team who already knew those databases existed. For the second identification it was helped by the Montenegro GRU suspect whose real and fake ID had been published. The team saw that a few specific details were shared by both identities such as first name, residence and date of birth. So began a process of elimination having found people within databases who share these details with the potentially fake identity of the other suspect, giving a pretty long list that was then whittled down by finding entries on that list on social media and verifying that they were genuinely a different person or cross-referencing them with other databases. This gave them an ever-decreasing list of potential identities until we eventually got to the passport document which we could then verify against other images and footage of the suspect.

Ears never tell a lie

The verification process involved looking at specific features on several images, one of which was a distinctive lump on the ear.

Carlo Ginzberg actually wrote about the use of ears for verification purposes in the 19th century when investigating art fraud, since often forging the earlobes in a portrait is where fake painters lose their concentration for a second and it can be a more telling clue for identifying forgeries than analysing other features.

Q

Isn't there a danger that these techniques can be used to propagate conspiracy theories?

A

Part of the reason Higgins started pursuing this practice was because this was already happening. One example is that of Kevin Dawes, an Asian American who travelled to Libya to become a journalist, but became 'evidence' that US soldiers were fighting alongside rebel troops there, despite Dawes not being and never having been in the US Army. So Higgins got involved in open-source, in part, to interrogate conspiracy theories.

A further example can be seen in a live stream from the capture of Tripoli, which was claimed to be fake since markings on a landmark were not visible on a screenshot from the video. It was claimed that this was evidence that the video was a fake, filmed on a set made up to look like Tripoli. But the real reason the markings couldn't be seen was the very low quality of the footage; it wasn't a conspiracy at all.

One of the problems with this claim was that there was no link to the original footage or source, so at least part of the answer to this danger is ensuring good practice in using the techniques such as including references to original source material.

Q

Can open-source investigation be used effectively in local contexts?

A

Bellingcat are working on projects to apply these techniques to local issues in both Amsterdam and Utrecht in the Netherlands. Another example came from a training event in London when Bellingcat trainer Christiaan Triebert was the victim of an attempted mugging by a moped gang. Making the best of a bad situation, Triebert turned this into a case study and the trainers and participants were able to find a huge amount of information by using court records and analysing social media profiles of the would-be perpetrators.

Forensic Architecture are currently using these techniques in an ongoing investigation of the Grenfell Tower fire, working with the G20, which is a group of lawyers representing the bereaved relatives and survivors. The problem they have is that the amount of information that exists is in hundreds of thousands of data

points. This includes all the people who were in and around the tower at the time of the fire including first responders as well as residents, their interactions and movements, phone calls, social media posts, etc. To investigate such a dense event in which 500 or more people are involved and each needs to have their own account necessitates a huge amount of analysis. So Forensic Architecture are building a spatial database system with a model that can navigate this in space and time. This includes mapping thousands of bits of footage showing the path of the fire into a continuous 3D representation, and a record of the movements and interactions which occurred. It's intended to be an evidential archive that can be used for any case, whether insurance or criminal.

The second part of the project is looking at the systemic history of the tower, mapping the changes that were made from the original building to identify if the incident was part of a longer-term systemic process. This work includes bringing together historical public documents, which detail the changes made over time, with other evidence such as images published in pamphlets by the company in charge of the more recent development.

Q

Is there a danger that in showing the methodology behind open-source investigation, you are making future investigations more difficult?

A

To an extent this is true, an example would be the recent Russian legislation banning soldiers from sharing images on social media. However, there's also constant innovation going on in the field, as well as plenty of legitimate investigative targets, whether individual people or nation states, who remain not as expert or careful as they would like to think.

Changes to social media platforms work both ways in regard to this. There have been many changes to Facebook in the wake of the Cambridge Analytica revelations, and all social media platforms are constantly developing and evolving anyway, but in most cases where methods are closed down other means of investigation open up, so there are always new avenues to explore.

Q

What about the potential for trauma in conducting this kind of work?

A

Bellingcat has recently published an article on vicarious trauma which provides a lot of best-practice and advice for minimising this risk and addressing the issue where it arises.

- Get to know yourself and your own sensitivities and triggers which will differ from person to person, especially where there is some personal connection between events being investigated or similar incidents.
- Prepare yourself mentally for viewing a potential trauma-inducing content and warn others appropriately before sharing such content.
- If you are working on content in foreign languages, learn to recognise some words that are likely to be associated with trauma-inducing content so you know what to expect.
- Be aware of and set limits on the environment in which you conduct the work. Keep it contained to an office. Alternatively, if you work from home keep it out of your bedroom, so that you have a safe space to return to when you need to rest. Set time limits and minimise work at night.
- There are also several simple technological steps you can take:
    - Mute your volume unless you absolutely need to listen; audio can often be more traumatic for people than imagery.
    - Use a thumbnail preview in the progress bar to give yourself warning of potentially traumatic content.
    - Consider using a sticky note or your hand to cover graphic images.
    - Always have autoplay turned off.
- Ensure a community and workplace culture that recognises the risks of secondary trauma, takes them seriously and allows enough flexibility, support and time for investigators to manage and address any symptoms of such trauma.

6

Protecting Stories

Sarah Giaziri
Laurent Richard
Pavla Holcova
May Jeong

Proceedings of seminars at
the third international
CIJ Logan Symposium

London, 19/20 October 2018

Goldsmiths, University of
London

Protecting Stories

If the intention behind violence and persecution towards journalists and whistleblowers is to keep their stories from ever getting out, and send a warning to others who may be considering researching similar areas, how best to protect the ultimate prize of investigative journalism: important stories?

In this seminar, Investigative Practice determined the methods through which journalists and their supporters can overcome the fear and intimidation that often causes them to drop investigations, or to never begin them at all.

Chair:

Sarah Giaziri
Director, Frontline Freelance Register

Panellists:

Laurent Richard
Founder, Forbidden Stories

Pavla Holcova
Organised Crime and Corruption Reporting Project (OCCRP)

May Jeong
The Intercept

> "It is flawed the way we think about journalistic ethics... we need to make sure our subjects make informed consent."
>
> May Jeong

There's a huge importance in forming a network around a story and the subsequent protection of the sources. Relationships with sources may change over the course of an investigation and there are many factors which affect this:

- It's worth taking your time to fully immerse yourself in the community on which you're reporting.
- Being based in a small community for a long time, everyone is likely to know you and your sources will be people close to you, so rather than calling a source for a quote once and then rarely speaking again, most of the stories you write in such a situation are continuations of an ongoing conversation you are having with the people around you.
- In May Jeong's case, her relationship with sources constitutes a large part of her social life.
- The conventions surrounding journalistic ethical practices ('on the record', 'off the record', speaking on background) only work for those who already have power. It is integral to the safety of the source to fully explain the risks and implications of their testimony.

Jeong has first-hand experience of following a story into danger (e.g. hiding in an Afghan army helicopter) and navigating the risks of a dangerous story is rarely an exact science. Such risks are often difficult to quantify, so you have to go with your instinct and your impression of the people around you. Most often, your gut is the thing that will keep you safe, but it's very important to have a reliable team or fixer, whose viewpoint you can trust.

In terms of more tangible precautions, Jeong recommends the International NGO Safety Organisation (INSO) to access security briefings every morning (the INSO is active in several countries and many other countries have equivalents). It is also advisable to seek expert opinions on certain stories, wherever you have a qualified contact, if you have been commissioned you should request a consultation with the outlet's security experts. The Frontline Freelance Register also advocates for risk assessments in such cases and provides resources to help to complete these.

"If a journalist is dying for one story, this story is likely to be very relevant to the public interest."

Laurent Richard

Laurent Richard started out as an investigative reporter working in several regions where there was a situation of conflict or repression of the press. The tragedy of losing friends in the *Charlie Hebdo* attack prompted Richard to start the organisation Forbidden Stories (which evolved from similar projects such as the OCCRP's Khadija Project and the Arizona Project), to help finish the difficult stories journalists started but could not finish due to threats, violence or murder. As the organisation was being set up, Daphne Caruana Galizia was murdered so they started work straight away, setting up the Daphne Project with 18 news organisations as partners.

The organisation aims to:

- Provide services to journalists to help protect their information and their stories.
- Help journalists most at risk who tend to work alone and publish through social media, as their stories are too risky for a newsroom. Forbidden Stories is tailored to these cases, helping them with tools from the open-source environment that they may not have access to or know how to use effectively.
- They propose using three main tools: Securedrop, Signal and PGP email.
- Allow journalists to publicly state that they have shared their story and evidence with Forbidden Stories as a disincentive to threaten or target them, since the story will still be able to be told. This is always decided on a case-by-case basis though, informed by a prior risk assessment.

> "A way of sending a message outside that you can't kill the story because there are five other people working on it, and they have access to all the data."
>
> Pavla Holcova

OCCRP protects journalists and their stories in a similar way by sharing the stories amongst a small network of people, including tech specialists who can ensure the security of the journalist's laptop. They also use 'OCCRP wiki', a platform like google docs, enabling reporters to protect their stories online, whilst sending a message that the story cannot be killed through their silencing.

They try and sustain the journalist's name in popular consciousness if they are imprisoned. Holcova gives the example of when the organisation signed off articles under the name Khadija Ismayilova while she was imprisoned. This produced enormous outside pressure, so that she was released from her seven and a half year sentence in a little over one year. However, it did have the effect of making her time inside more difficult as the government believed she must be publishing stories from her cell, and subjected her to room and strip searches.

Q

If you receive a violent threat, are there tools to test its legitimacy?

A

Pavla Holcova argues that journalists tend to underestimate threats. They think that if someone is openly threatening them it means they are unlikely to actually follow through, but this is often a mistake. It is important to take threats seriously and perform an evaluation of the seriousness according to what the story is, the context the journalist is working in and the likely sources of the threat or threats. It's also important to take personal and online security precautions, to see if someone is following or tracking you and to mitigate the risks of that. The vast majority of murdered journalists are physically followed beforehand.

For Richard, the key is teamwork. His experience, having been arrested in Azerbaijan, was that his safety was increased by being aware that it was likely to happen and having already connected with the French embassy and his editor in Paris. He had previously backed up his information with someone he could trust and had constructed a Communications Plan in which he figured out what tools he was going to use to continue communications with sources. This meant that the reaction time was quick and he was out before charges could be pressed. Anticipation is hugely important, especially as the first few hours after arrest are key, so that you can access outside help from organisations or embassies before the situation is formalised and charges are brought.

It can be difficult when freelancing without the support of a news organisation behind you, but it is sometimes possible to consult people from other news outlets (Jeong often contacts The Intercept in this regard). Ultimately though, the most important thing is to follow your gut: 'what do your instincts say and with the people you respect, what do their instincts say?'

Sarah Giaziri highlights organisations that work in this area and produce resources that can help to evaluate the legitimacy of threats. For instance, Reporters Without Borders (RSF) and the Committee to Protect Journalists (CPJ) have local partners and experts in many countries as well as a central assistance desk which can help with such an evaluation. CPJ also have an emergency response programme which can connect you to a security consultant with which you can have these kinds of discussions and access expert advice. The Rory Peck Trust and Internews also provide tools and resources on how to report and assess threats. Much of this is focused on conflict journalism, but there are training programmes that focused more on security for investigative journalists as well.

However, pre-emptive training is usually more effective than support after the fact, so journalists should try to spend time preparing beforehand as far as possible.

Q

What do you do about a real physical threat?

A

After an evaluation of the risk, if it looks like a real threat then OCCRP will get a reporter out of the country, leaving without their technical equipment, to ensure they are not being tracked.

Organisations such as RSF and CPJ also have some funding available to provide journalists under threat with safe housing. This can cover a few nights in a hotel in situations of immediate threat, during more sustained threat situations they can provide help in accessing fellowships for a few weeks or months. They are often overwhelmed though, so to ensure that your request for help is recognised as urgent when it reaches their desk, it is recommended to be in contact with the organisations representative in your country before the situation becomes critical.

There is also a wider network of organisations with access to emergency funds for these purposes, who collaborate on allocating this money, including Free Press Unlimited. Again though, it is key to be in touch with representatives from these organisations and report regularly on your situation so that they can prioritise your request when required.

Q

When protecting a story, do we value the reporter, the story itself, or we do think purely in terms of its impact?

A

“No story is worth dying for” is an oft-repeated maxim, but actually the incentive structure for a working reporter is the opposite. The worth of a story is essentially a philosophical question eg. do you believe in the greater good or do you believe in individual autonomy? This is a decision people need to make on an individual level. But it is definitely true that the way the industry is currently structured will always reward reporters more for taking immense risks.

Holcova believes that if a reporter is in danger they should always be prioritised and another way should be found to finish the story. For instance, a solution can be that another journalist working in a different country is enlisted to continue the work and publish remotely but still keep the impact within the country of concern.

Q

How do you deal with the psychological impacts of long-term surveillance?

A

The solution is finding a balance. There are so many pressures that come with the job: lawsuits, social media threats and the expectations of individuals around the story, and it is important to draw certain lines for the sake of yourself. Holcova gives a personal example of deciding not to live under police protection after the murder of a colleague because it was too much of a psychological strain. This will always depend on the individual capacity and coping mechanisms of each reporter though.

There are organisations that offer psychological support to journalists, such as the Dart Center. They have an international team who provide psychological support to journalists dealing with traumatic events. It is important to recognise trauma and deal with it appropriately, not just because of the mental health implications, but also due to the risk of making poor decisions when working under the impact of trauma. There are many self-care processes that you can put in place and the Dart Center provides resources and tools to help with these.

It's worth remembering that you need to be in the right place to talk to a psychologist; it's not always helpful to speak to a psychologist straight away. The Dart Center runs online sessions for psychological care in several languages, although there are limits to the benefit of such support when accessed online. The Center does also have a network of psychologists in many countries so they do have the capacity to provide face-to-face support as well.

One other element which adds to the pressure of working under surveillance is the responsibility that journalists have for the protection of their sources. These people are more at risk from the surveillance, as they are usually taking more direct risks in speaking to journalists and they are also much less likely to have access to tools, resources and support for ensuring secure communications and avoiding the risks of being surveilled. The main way to help mitigate this pressure is again preparation and familiarising yourself with the tools and techniques so that you can do as much as you can to help your sources.

There are also psychological threats that come not from surveillance but from the difficult issues with regards to the media's role in the growth of groups that rely on violence and terrorism. This is a paradox of the journalism industry; by reporting something you are affording it a certain level of credibility. It can sometimes feel like we are merely inoculating the public to superlative statements through constantly upping the ante in the ways in which we report certain events. There is a risk that journalists, especially conflict journalists, end up feeling complicit in increasing cycles of violence. This is a different, more philosophical problem which puts journalists under pressure, and while there does not seem to be an easy solution, it is an issue which requires more thought and consideration.

7

Source Code

Silkie Carlo
Joseph Cox
Marie Gutbub
Fabio Natali

Proceedings of seminars at
the third international
CIJ Logan Symposium

London, 19/20 October 2018

Goldsmiths, University of
London

Source Code

Information security is now an established weapon in the fight to keep journalists and their sources safe, but are we in danger of encouraging people to rely on technology that they might not fully understand, thus putting them at greater risk? Are we losing sight of the traditional way in which journalists keep their sources safe – by being unpredictable, and by using our wits as much as our smartphones?

In this seminar, Investigative Practice identified ways to combine the old and new in journalist operational security, as well as how best to advise whistleblowers who might want to send journalists and media outlets their stories.

Chair:

Silkie Carlo

Director, Big Brother Watch

Panellists:

Joseph Cox

Technology journalist at Vice's Motherboard

Marie Gutbub

Infosec Trainer and Nextcloud

Fabio Natali

Director, Reckon Digital

> "It is more important to understand the underlying concepts than the tools themselves."
>
> Joseph Cox

A combination of old and new technology can be used to keep information safe. Tor and Signal are effective tools, but often journalists are unaware of how they work and what they are doing. Likewise, due to a lack of expertise, if a journalist is hacked, they are unlikely to identify what malware is being used. As such, rather than focusing on what apps and operating systems are available, we should focus on what these technologies are doing. In doing so, it will not only enable journalists to use such tools more effectively but also make them more receptive to how those tools may change in the future.

There are various concepts that are worth understanding:

1. Compartmentation: separating information into distinct cells - e.g. using a specific laptop to access leaked information, that you don't connect to any accounts linked to you, or ideally don't connect to the internet at all.

2. Concealment: encrypting communications via PGP or Signal

3. Cover and Counter: The process of creating superfluous information to distract from what you want to hide - for example, by arranging a fake encounter whilst the real encounter occurs elsewhere.

> "Many media outlets are yet to understand that that they need to hire IT staff who can work with operational security in mind."
>
> Marie Gutbub

News outlets may be reluctant to trust journalists or to acknowledge the need for an infosec expert, which can cause problems. For instance, Marie Gutbub recounted an example of a German journalist who used PGP when doing a story involving local activists. The in-house IT assistant refused to give him admin rights or let him use his company address on his private computer. This is a case where the outlet should have trusted the journalist's understanding or referred to a specialist.

There are not many workarounds for this, especially if you are unable to use a private computer, but journalists can use non-work email addresses for communicating with sources and then use private computers, though that can cause problems with compartmentalisation. In some cases, journalists should buy a separate computer for this purpose, though this obviously also has cost implications.

However, the better method to counter this problem is probably to push back against restrictive IT policies in your newsroom and start an argument (or ideally, a discussion) with your editors about the benefits of either allowing some admin rights to journalists on work machines, some flexibility over using organisational email addresses on personal laptops, or teaching IT staff about the importance of information security for the purposes of source protection. This method has the added advantage of helping your colleagues and other journalists that come to the newsroom after you, and hopefully starting to change the newsroom culture more generally.

> "Transparency means making the inner mechanisms of technology more visible."
>
> Fabio Natali

On the one hand, digital technologies can be very convenient and helpful but on the other hand, they may add a layer of opacity. There is an argument for trying to make these technologies more transparent, to improve the users' experience of applications and tools. This may also include broadening knowledge about the infrastructure of certain applications, making algorithms and machine learning easier to understand, for instance. That said, as digital citizens, we should work to further our own understandings of technology; through workshops, events, training days and reaching out to experts.

At the moment, journalists often tend to seek out training when they are covering a story that demands secure communication lines. There needs to be a conceptual shift that has to happen earlier on in the process so that this knowledge gathering is taken as a pre-emptive measure rather than used as a last resort.

To achieve this conceptual shift, it's essential for training in information security to take place in journalism schools. Catching future journalists at the point where they are at their most open to learning new tools and acquiring new skillsets. Journalists who are currently working are generally too busy and overwhelmed with the work and other skills and tools they feel they need to learn.

On the level of editors, one of the most effective ways of explaining the need for information security tools and skills for their journalists is as a cost-saving exercise. This argument works on two levels, partly because the majority of the software taught is open-source and therefore largely cost-free aside from the time and training requirements to implement and use it effectively, but also as insurance against the major risks of having poor security infrastructure and compromising both the data and the sources of the journalists in their newsroom.

Q

Could we operate without any technology tools at all given how insecure technology often is?

A

We can, but in today's world we would massively handicap ourselves if we avoid digital technology entirely. There is of course a similar danger of handicapping ourselves unnecessarily by placing too much importance on only ever using the most secure versions of digital technology.

Journalists tend to think that their story (and sometimes themselves) are more important than they actually are. On the majority of stories tools like Signal or Tor aren't strictly necessary. Far more important in general practice are basic security measures like two-factor authentication on your accounts and using strong passwords.

The most critical process in this regard though, is threat modelling. Anyone considering information security needs to go through an assessment to identify what it is that requires protection, who to protect it from and what their surveillance capabilities are likely to be. Without thinking this through, journalists are in danger of placing their information security needs in the wrong place of a spectrum between user-friendly but insecure tools, and tools with better security but higher technical requirements.

There is also a danger in training journalists about information security without placing enough importance on threat modelling that we perpetuate 'security nihilism' in which subjects start to feel overwhelmed by the range of security vulnerabilities and end up feeling defeatist about securing their communications rendering the training actually counter-productive.

Q

There is a risk of being red-flagged simply because of the use of certain tools like PGP or Signal, which is especially compounded when working with people across international borders. In certain national contexts this presents a bigger targeting risk than communicating about sensitive issues through unencrypted means. Can we safely advise others we work with to upgrade their security tools, essentially assuming a better knowledge of their threat model than they have themselves?

A

It's certainly true that use of some tools can cause trouble for people in particular countries and it's always best to assume that they know what their targeting risks are better than you. The security of the source should always be of primary importance, which in some cases means killing the story if need be or taking a step back until a safer and more secure path of communication can be established. It may also mean seeking the expertise of lawyers and specialists.

There is some cause for positivity here though, with the increasing ubiquity of end-to-end encryption as in tools like Whatsapp. The more people who are communicating with end-to-end encryption, even with non-open-source software, the less likely authorities are to see this as evidence for suspicion.

Carlo summarised the recommendations from the discussion:

- It's important for us to increase our understanding of technologies, attend events and workshops, creating a network of technology experts around us that we can fall back on.
- Media outlets have to realise that IT staff should know the importance of source protection, or trust their journalists with admin access on workplace computers.
- Having conferences such as this where there are dedicated workshops on security are great for raising awareness of the issue.
- Teach journalists the basics of security whilst they're still studying journalism when they're more likely be in the mindset to learn, unlike working journalists who have little time.
- Create a 'pincer movement' to target the people who are learning journalism but also persuade editors to ensure their journalists are equipped enough to be secure.
- Sell the importance of information security to editors through the idea that it is going to save them money in the long run.

In general people should look for open-source software, so that the code is available for independent audit. There are also resources and software available for guidance when conferences and training workshops are inaccessible:

- InfosecBytes CIJ video tutorials for core security tools.
- Little Snitch can be used to monitor apps, preventing or permitting them to connect to attached networks through advanced rules.

- Security First produce Umbrella, a digital security handbook in a secure open-source app for Android and iOS.
- Security without borders publish updates and briefings on hacking and information security.
- National Cyber Security Centre These UK government security guides do actually contain some useful security advice to protect yourself from low-level attacks (though obviously if you're investigating the security services, you may want to use more secure tools).