It used to be possible to promise confidentiality to sources – guaranteeing protection of their identities, even on pain of jail – in countries where legal source protection frameworks were robust. But, internationally, ethical commitments to, and **legal protections** for, journalistic sources are being **undercut** by surveillance (both mass surveillance and targeted surveillance), and mandatory data retention policies; **trumped** by national security and anti-terrorism legislation; **undermined** by the role of third party intermediaries (like social media and search engine companies, telcos and ISPs), and **restricted** by overly narrow interpretation of laws designed for an analogue world. So, the attention of investigative journalists and their editors is necessarily turning to **risk assessment, self-protection** and **source education.**

PROTECTING SOURCES IN THE DIGITAL AGE

Investigative journalists struggling to uphold their ethical commitment to protect their sources in the digital era are changing their practices significantly as the Snowden effect takes hold in our newsrooms. For many journalists, "going back to analogue basics" is the new normal when dealing with confidential sources. **Julie Posetti** examines the evolving issues as they emerged during recent interviews with over two dozen leading editors, investigative journalists and media lawyers.

How much confidence do investigative journalists have in the ability to protect sources in 2015?

At the time of our interview in his London office in late January 2015, outgoing Editor-in-Chief of The Guardian Alan Rusbridger was despondent about the threat to investigative journalism posed by the erosion of source protection. "Well, I'm very gloomy," he said. The limitations on existing legal frameworks supporting source protection in the UK are coming thick and fast. It's like fighting a "Zombie War," he said, waving his hands in exasperation.

Rusbridger has previously suggested that investigative journalism may not be possible in the post-Snowden era. That's a concern shared by Committee to Protect Journalists' Global Advocacy Director Courtney Radsch: "I think that we are really potentially looking at an environment where it becomes virtually impossible for journalists to protect their sources – where journalists are no longer even needed in that equation, given governments' broad surveillance powers."

Bolivian investigative journalist Ricardo Aguilar is seriously concerned about the reliability of legal source protection. He was charged with espionage and threatened with 30 years jail after refusing to reveal his source on a 2014 La Razon story. "Mass surveillance, data retention and the appeal of (the) National Security category leaves the protection of secret sources in latent vulnerability," he said.

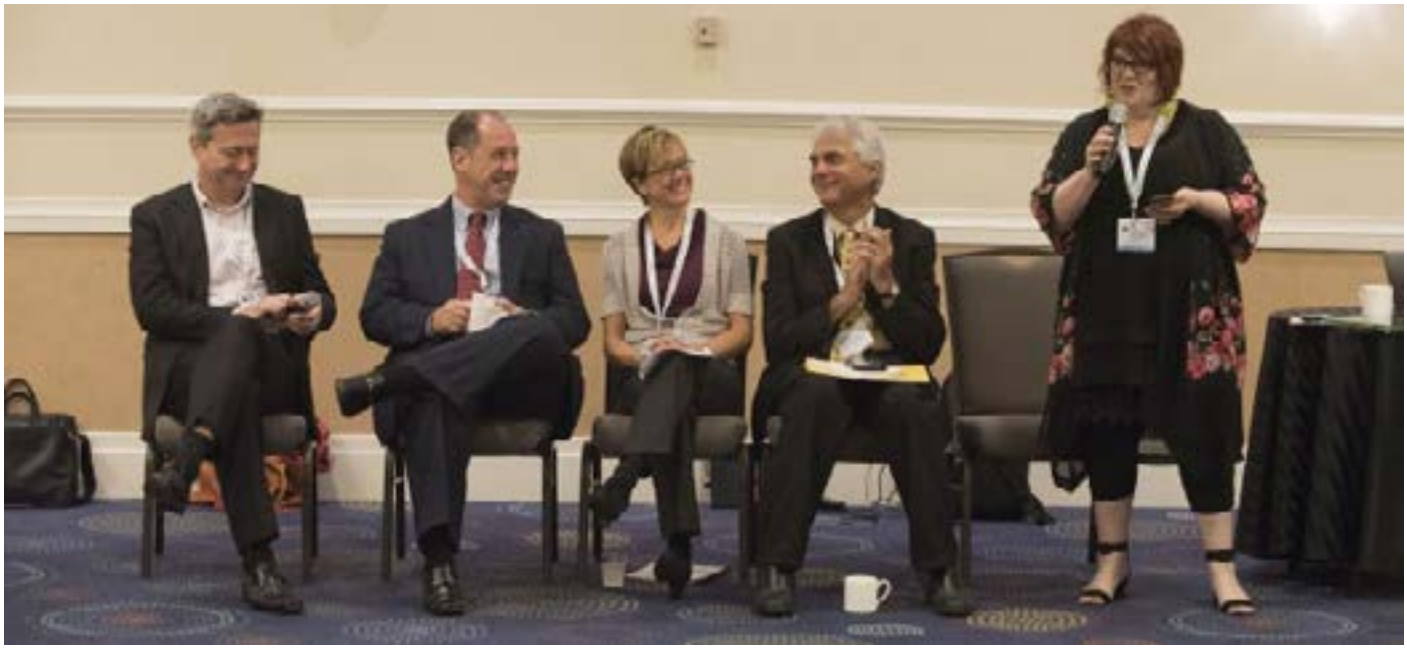
Director of the US-based International Consortium of Investigative Journalists (ICIJ) Gerard Ryle is similarly direct. "I'm not confident that there is any protection at all, to be frank... I would say as a general rule these days, much more than in the past, it's very difficult to protect sources because of the fact that electronic communications can be back-tracked and people can be found much easier than they may have been found in the past," he said. Ryle, who oversaw the global investigative journalism projects known as Offshore Leaks, Luxembourg Leaks, and Swiss Leaks, once faced the threat of jail in Australia while reporting on police corruption for The Age, after refusing to give up a source to an ombudsman's inquiry.

In Sweden, where source protection legislation is so strong that journalists can be jailed for revealing their confidential sources, top investigative journalists are taking extraordinary measures to protect them from the impacts of mass surveillance, and other risks of the digital era. One of the threats identified by the director of the investigative unit at Sweden's national public radio (Sveriges Radio), Fredrik Laurin, is the risk of police seizing digital content due to gaps in source protection legislation in his country: "It's not an exception – this is definitely the modus operandi. The police, they don't go into newsrooms very often here, but when they do they have no problem in grabbing digitally stored information."

The chilling effect

Co-founder of Pakistan's Centre for Investigative Reporting, Umar Cheema, believes his status guarantees that he is under surveillance and his sources know it. "I am a prominent journalist, a distinction with its own advantages and disadvantages. Some [sources] tend to approach me out of respect and belief that I am the right person to be taken into confidence. Others hesitate, fearing any contact with me will put them on [the] radar screen since I am under surveillance, right from phone to emails, and [my] social media accounts are monitored."

Cheema was kidnapped and tortured in 2010. In the course of his captivity, his sources were compromised. "The captors, who I strongly suspect belonged to our premier intelligence agency, took away my mobile phone, apparently for investigating



Julie Posetti launches preliminary findings from the study with Guy Berger, Amy Mitchell, Charles Tobin and Gerard Ryle

in detail about my professional contacts through my phone contacts," he said. "Some of my sources, who had shared information about national security, were coerced into silence. They never contacted me after- wards, other than telling in brief... about the harassment they had to face." Cheema said that threats to his safety sent via phone and email are now routine.

International Editor of Algeria's El Watan newspaper, Zine Cherfaoui, said sources now increasingly require face-to-face meetings. "Since Snowden and mass surveillance, sources speak with difficulty and people don't have as much confidence. To really discuss with people we prefer to avoid electronic means or social networks. The Snowden Affair turned upside down the work of journalists... It's harder to speak to people. We really have to go out and meet them. It's face to face," Cherfaoui said.

However, it should be noted that the risk of exposure travels with journalists heading to face-to-face meetings with sources if the route they take is subject to security camera surveillance, or they travel with traceable mobile devices that deliver geolocation data.

At the time of my interview with Rusbridger, The Guardian was in the midst of a major tax investigation, and the paper was being challenged by approximately 20 companies of solicitors over it. "They're all wanting the return of documents, they're all citing data protection laws, privacy, everything... so the bills on these things just mount and mount and mount and mount, so you can easily be spending tens or hundreds of thousands of pounds trying to get a story into the paper."

"Of course, once you get onto secure reporting there is a significant cost... in trying to create a safe environment where we feel we can offer our sources the kind of protection that they deserve", Rusbridger says. The cost of digital security technology, training and legal fees connected to source protection in the post- Snowden era also represents a significant chilling effect on investigative journalism. The Guardian spends about a million pounds more a year on legal fees than they did five years ago, according to Rusbridger: "It's definitely having a bad effect on the overall ability to report," he says, pointing to the devastating impact of the changed landscape on regional newspapers, in particular. "(They) can't afford to get tied up in defending their staff, or equipment, or the IT," he said.

But isn't this a golden age for investigative journalism?

"Technology is allowing information to be leaked on a vast scale... For me as a journalist we're in boom times, because you're able to get information that's incredibly detailed and you're able to get stories that you couldn't possibly [get before]," ICIJ's Gerard Ryle said, declaring the digital era a "golden age for journalism," despite the risks.

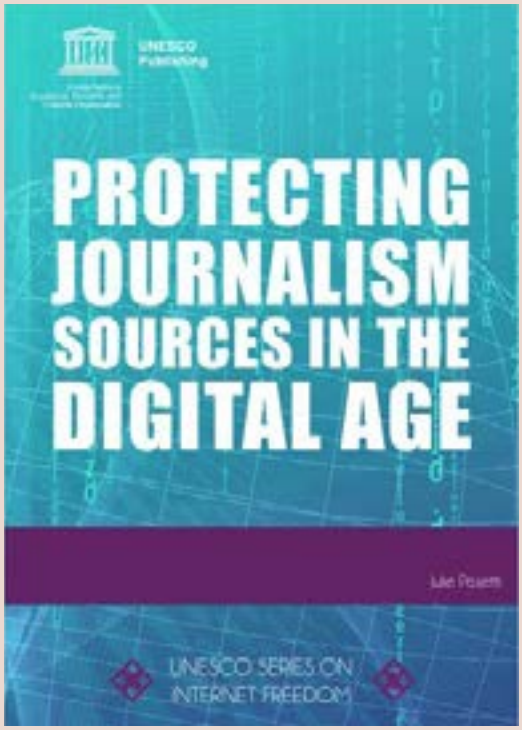
Prominent Jordanian investigative journalist and founder of the Arabic Media internet Network, Daoud Kuttab, echoed Ryle's view of the digital era: "On the one hand I think it has accelerated and widened the amount of data available to everyone and made it very easy to transfer information and documents. Now you can put thousands of documents on a USB so you don't have the problem of having to carry things out of offices – you can email, send as an attachment. But at the same time governments are able to invade your privacy much easier and get information."

Editor-in-Chief of Argentina's La Nacion, Carlos Guyot, also acknowledged the significant benefits of digital era investigative reporting involving confidential sources, including access to leaked documents that would have been impossible to get even five or ten years ago. "New technologies

A plan for protecting journalism sources in the digital age

A major output of the study is an 11-point assessment tool for measuring the effectiveness of legal source protection frameworks in the digital era. It was concluded that a model framework should:

1. Recognise the value to the public interest of source protection, with its legal foundation in the right to freedom of expression (including press freedom), and to privacy. These protections should also be embedded within a country's constitution and/or national law
2. Recognise that source protection should extend to all acts of journalism and across all platforms, services and mediums (of data storage and publication), and that it includes digital data and meta-data
3. Recognise that source protection does not entail registration or licensing of practitioners of journalism
4. Recognise the potential detrimental impact on public interest journalism, and on society, of source-related information being caught up in bulk data recording, tracking, storage and collection
5. Affirm that State and corporate actors (including third party intermediaries), who capture journalistic digital data must treat it confidentially (acknowledging also the desirability of the storage and use of such data being consistent with the general right to privacy)
6. Shield acts of journalism from targeted surveillance, data retention and handover of material connected to confidential sources
7. Define exceptions to all the above very narrowly, so as to preserve the principle of source protection as the effective norm and standard,
8. Define exceptions as needing to conform to a provision of "necessity" and "proportionality" — in other words, when no alternative to disclosure is possible, when there is greater public interest in disclosure than in protection, and when the terms and extent of disclosure still preserve confidentiality as much as possible
9. Define a transparent and independent judicial process with appeal potential for authorised exceptions, and ensure that law-enforcement agents and judicial actors are educated about the principles involved,
10. Criminalise arbitrary, unauthorised and wilful violations of confidentiality of sources by third party actors
11. Recognise that source protection laws can be strengthened by complementary whistleblower legislation.



Download pdf

The study responds in part to acknowledgement in both the UN General Assembly and the UN Human Rights Council of "the particular vulnerability of journalists to becoming targets of unlawful or arbitrary surveillance or interception of communications in violation of their rights to privacy and to freedom of expression." It also contributed to a global UNESCO study of internet-related issues.

The preliminary findings were launched during a Pew Research Centre-sponsored breakfast at the World News Media Congress today, during which Pew Journalism's Research Director Amy Mitchell joined the Director of the International Consortium of Investigative Journalists Gerard Ryle, UNESCO's Director of Freedom of Expression and Media Development Guy Berger, senior DC media lawyer Charles Tobin and Julie Posetti. Other researchers who contributed to the study are Dr Marcus O'Donnell (University of Wollongong), Professor Carlos Affonso Pereira de Souza (Brazil), Professor Ying Chan (China, Hong Kong), Doreen Weisenhaus (China, Hong Kong). Lead Research Assistants were: Federica Cherubini, Angelique Lu and Alice Matthews.

bring new challenges with them, but also new opportunities, like encrypted conversations via new software, although this must be combined with old fashioned practices... there is nothing like a face-to-face meeting with a source," he said.

However, one of the risks of this data-boon is the rush to legislate against the impacts of leaks, according to Gerard Ryle. "The leaks are getting bigger, therefore the law is scrambling to catch up... and that's the danger for authorities, and for people who want secrecy, and I think that there is a push generally across the world to try and cope with this," Ryle said. "[It's] a problem for governments, agencies, any organisation that wants to keep secrets. It's becoming more and more difficult to keep those secrets."

Just assume you're being watched

How do reporters protect their confidential communications with sources in the age of surveillance? "I'm more careful with any digital platform that I'm involved in – whether it's email, phone or any other digital format. I assume that [I am] probably being watched, listened to, or read. That's my starting point and I take it from there," Daoud Kuttab said.

ICIJ's Gerard Ryle adopts the same mode. "I just assume that it's possible to collect that kind of information, and you work in that environment, and you just assume that all your emails, any form of communication, is potentially found out and so I just be sensible about it. Don't put things in writing, don't do certain things if you don't want them to come out afterwards. You have to assume that everything you do is being recorded or traced."

A change of practice in managing digital communications is required in response – at both the personal and professional levels – according to Deputy Director of the Tow Centre for Digital Journalism, Susan McGregor. "It means that we have to be thoughtful about our devices and our communications in the way that most of us aren't accustomed to doing yet... Some of the habits we've developed as private individuals, taking our phone everywhere, always having wifi on, emailing everything, we're just going to have to think differently about those things when it comes to working with sources," she said.

Going back to basics

Alan Rusbridger has despaired that investigative journalism based on confidential sources may not be possible in the digital age, unless journalists go 'back to basics': "I know investigative journalism happened before the invention of the phone, so I think maybe literally we're going back to that age, when the only safe thing is face-to-face contact, brown envelopes, meetings in parks or whatever," he said.

UK QC Gavin Millar, who has advised The Guardian, tells his clients to revert to traditional methods of investigative journalism. "They actually have a contract phone and throw it into the Thames at the end of each week, they will meet sources in pubs, write notes, hide the notes. In notebooks, in distant places where people can't get them if their houses are searched by police and some of them are very, very good at it."

Bolivia's Ricardo Aguilar avoids using digital communication in order to protect his sources. "Extreme distrust is the only defence against the possibility of a raking of secret sources in email accounts or social networks," he said. And La Nacion's Carlos Guyot says his investigative journalists are spending a lot more time on the road now. "...Our main investigative reporter drove for three hours to a different city for a 15-minute conversation with a source, and drove back to our newsroom. If we are willing to endure the challenges, we can still do good journalism."

New technologies bring new challenges with them, but also new opportunities, like encrypted conversations via new software, although this must be combined with old fashioned practices... there is nothing like a face-to-face meeting with a source.

El Watan's Zine Cherfaoui said journalists in the Middle East and North Africa have also reverted to face-to-face meetings with confidential sources, being particularly concerned about email communication. "We've become very cautious with social networks and everything that is electronic. Generally, we prefer to meet the source in person when it is very important. Because of mass surveillance and new anti-terrorism laws we like to avoid social networks."

Swedish Lawyer and Press Ombudsman, Par Trehorning agreed: "I've talked to a lot of editors and the best thing to do today is to write an ordinary letter. Email I think is most dangerous because it passes so many hands, (if) it is not encrypted. It's like a post card." Three journalists interviewed for this chapter mentioned the trend of relying on chat-apps as a more secure form of source interaction than email, but Mexican journalism safety expert Javier Garza Ramos warned against such an approach. "If we're sloppy and we say everything we know about our sources on our Gmail and on our WhatsApp, then of course the government is going to find out who our sources are, or whoever is spying on us," he said.

Simple approaches like stretching the timeline between contact with a source and publication of their leaks can also be used to disguise connections and minimise the chance a source will be "caught", Gerard Ryle said. "I mean the more layers you can put between you and the source sometimes is better, and a lot of that is time... if someone gives you some really hot information, the temptation is to publish that right away, but that's also when your source is potentially at most risk."

Taking responsibility for digital security

In 2015, it's not just lead investigative journalists and war correspondents who need to deal with digital era threats to source protection, according to Alan Rusbridger: "It's become increasingly hard to report on the national health service because you know they all have confidentiality agreements, so if you're a health reporter you probably want to make sure that you begin to understand this stuff."

The other factor to consider is that seemingly innocuous local stories built on anonymous sources can turn into large-scale investigative journalism projects. From little stories, big stories grow. But careless initial contact with a source makes such a person increasingly vulnerable as the story develops.

Swedish public radio's Fredrik Laurin said journalists are underdeveloped when it comes to protecting sources in the "digital hemisphere." "Very few journalists use encryption and very few journalists even know how to use it – it's not in their toolbox and that is a major problem," he said. "And when you do come into contact with sources... you often get confronted with very important questions – how do you, in reality, protect this source? Are you going to store the information on the company server? How are we going to communicate? I cannot use my corporate phone, for example. What level of encryption do you use? Serious questions." According to Laurin, his team's digital security expertise gives them an edge in journalism based on confidential sources. "(W)e are some of the few people in the journalistic community who actually employ encryption and who are trying to get wise on these issues and keep up with that."

Laurin's hardcore dedication to digital security in the interests of protecting his sources may seem extreme, but it needs to be understood in the context of the Swedish legal source protection framework that actually criminalises unauthorised source revelation. "It's me, Fredrik who goes to prison if you are my source and I lose my notebook, my note pad at the bar and your name comes out because of that. That's my fault and I go to prison. That's why I don't use Gmail for example. Or Facebook," he said. And Laurin also bans his staff from using Apple products because of concerns about security weaknesses connected to Apple devices revealed by Edward Snowden. "I need to survey – which I do, very thoroughly – who my suppliers are. I know exactly where my server is standing, I know exactly what the contract says, the hard discs in that server are named in my name, with my phone number. There's a tag on the material that says this material is protected according to the Swedish constitution."

However, ICIJ's Ryle, who remains utterly optimistic about the future of investigative journalism in the digital age, despite the threats to source protection that he acknowledges, said that too many journalists are growing unnecessarily paranoid. "There are some reporters I know (who are) completely paranoid about their computers – they're fantastic at encryption, everything is offline. But so what? Most of what they're working on isn't relevant."

Another issue to consider: digital security measures designed to protect sources can be unwieldy and time-consuming, and these factors remain a deterrent to many investigative journalists. "When we were doing the Offshore Leaks project we started off by trying to encrypt a whole email communication with everyone we were working with, it became a complete nightmare, because, first of all not all of us are very technological, including myself, and it became a hindrance to communication," Ryle admitted.

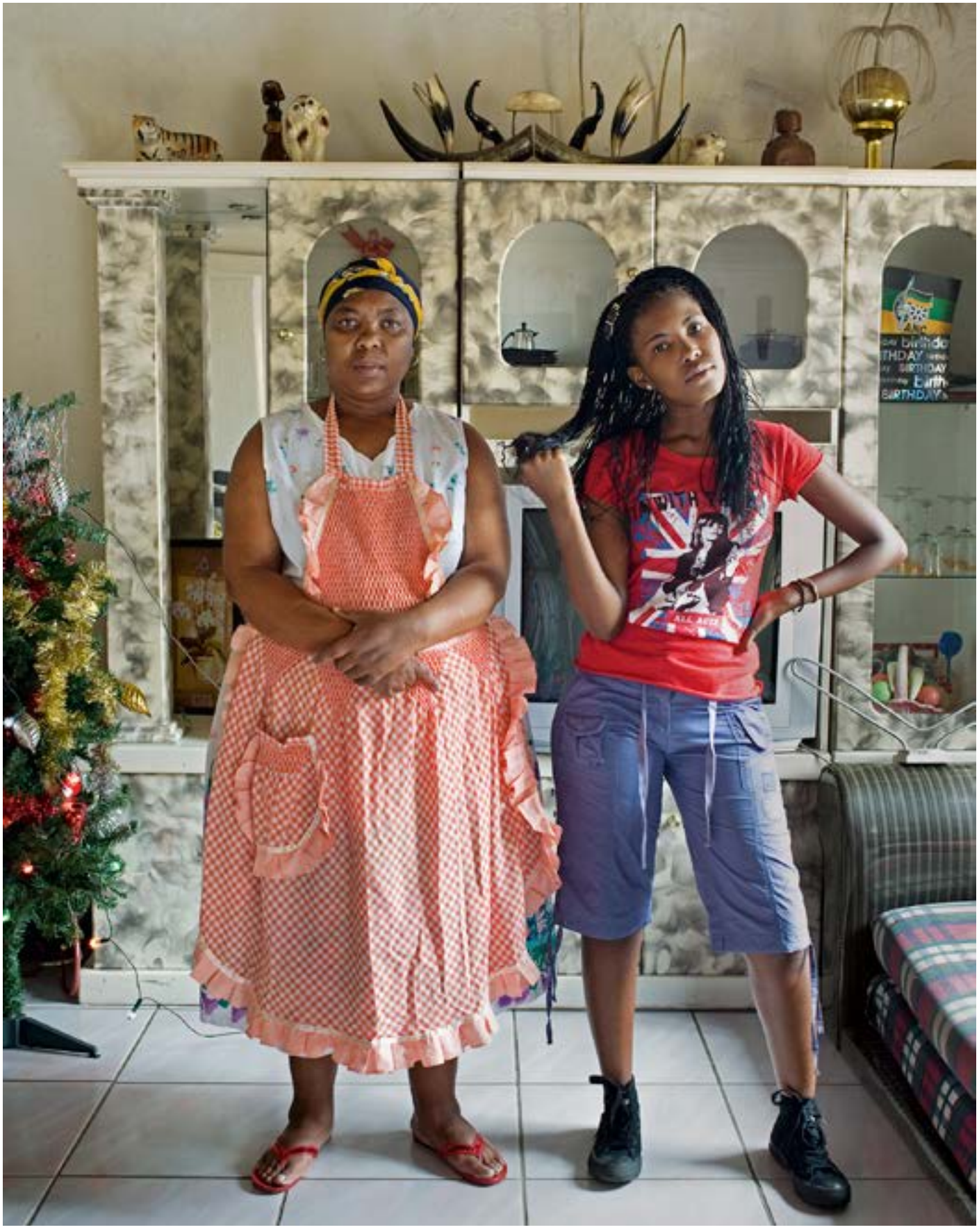
Journalists need training in digital security, but so do their sources

There is a new trend emerging in reference to source protection: journalists are beginning to train their sources in digital security to help them ensure their anonymity. La Nacion's Carlos Guyot said: "If we want journalism to survive and flourish in the 21st century, there is no other option than give our reporters, and sources, the tools necessary to do their jobs."

Alan Rusbridger acknowledged this challenge. "But because often sources are of interest to people with access to surveillance equipment, corporate or government, it feels like an unequal battle really."

However, as Executive Director of Arab Reporters for Investigative Journalism Rana Sabbagh pointed out, even the best training cannot keep up with global intelligence services: "We train our journalists in encryption and how to protect their data, and tell them to always assume that everything you're doing online, on your computers, is accessible, because even if you give them the best software and training, the intelligence agencies are always a step ahead.

How do you, in reality, protect a source? Are you going to store the information on the company server? How are we going to communicate? What level of encryption do you use?



Soweto by Jodi Bieber

They are using the latest technologies to decrypt the content, they are using technologies coming from countries that are supposed to protect free speech like the US and Switzerland."

Nevertheless, encryption may buy time in the course of an investigation, and it may at least keep other potentially hostile actors at bay – even if not the intelligence agencies.

Outsourcing source protection

In its global investigations that involve myriad international publishing partners, ICIJ essentially becomes the source: "By taking all the responsibility of source protection and also putting the responsibility on each organisation to do whatever it is according to their own laws. So we don't take responsibility for the publication of our projects in each country, each organisation has to do that, but in terms of giving them the information, we become the source... in other words we give them the documents... ICIJ is the source of the material," Gerard Ryle said.

Meanwhile, international news organisations have begun collaborating on platforms designed to securely receive digital information from confidential sources.

AfriLeaks, for example, is a Pan-African project that uses a highly secure mailbox designed to receive leaked documents, which connects investigative media houses to whistleblowers. It's operated by the African Network of Centres for Investigative Reporting. And, in Mexico, Mexicoleaks launched recently.

Sourcesure and Balkanleaks are similar Francophone and Bulgarian websites that allow whistleblowers to upload secret documents anonymously. Sourcesure, which is based in Belgium, to take advantage of strong source protection laws there, was jointly established in February 2015 by France's Le Monde, Belgian publications La Libre Belgique, Le Soir de Bruxelles and RTBF (Radio Télévision Belge Francophone). Yves Eudes, Sourcesùre's co-founder and a journalist at Le Monde, believes that the cross-border, multi-platform collaboration between leading Francophone news organisations is a spring of immunity for journalists and their sources against coercion. "Unity is strength. This initiative could not have been launched by Le Monde or RTBF alone. Sourcesùre is underpinned by a whole spectrum of collaborators, from liberal to conservative media outlets, united by common journalistic values," he said. Sources using the system are encouraged to download TOR software at their end before connecting with the system.

Ultimately, is it sustainable to promise confidentiality to sources in an era when it is so easy to identify a source without the involvement of the journalist, especially considering it can be a life or death matter? ARIJ's Rana Sabbagh is clear in her response: "Even in the best and most democratic of countries, one can't promise that anymore. There is no 100% guarantee."

This case study appears in the World Editors Forum's Trends in Newsrooms 2015*, which is free for members to download.*
Protecting Journalism Sources in the Digital Age *is published by UNESCO. Also see* Building digital safety for journalism.

Seven tips to help make your sources more secure

- **Don't grow unnecessarily paranoid – instead act smarter, get properly equipped and go back to basics where necessary.**
- **Be aware that even face-to-face meetings can be compromised by the presence of geolocatable mobile devices and security cameras.**
- **Assume you're being watched.**
- **Encrypt your data.**
- **Be aware that using Tor, PGP and other forms of data encryption can 'red flag' digital communications with sources (such practices can make you and your sources a bigger target).**
- **Recognise your ethical responsibility to protect your sources and consider training your confidential sources in digital safety and security.**
- **Recognise that it may no longer be possible to guarantee protection for your confidential sources and consider the ethical implications of that realisation.**

Julie Posetti wrote this report as a Research Fellow with the World Association of Newspapers and News Publishers (WAN-IFRA) based in Paris, France. She lectures in broadcast, multimedia and social journalism at the University of Wollongong, Australia. She's been a national political correspondent for the Australian national broadcaster, the ABC. She is writing a PhD thesis on "twitterisation of journalism". jposetti@uow.edu.au