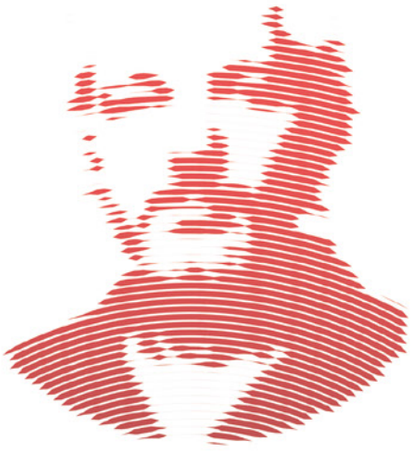
EPFL

THE C4DT

January 2022

C4DT Focus N°2



Protecting journalists and their sources

Featuring interviews with:

Pierre Romera
CTO of the International Consortium of Investigative Journalists (ICIJ)

Carmela Troncoso
Head of the Security and Privacy Engineering Laboratory at EPFL

Written by Daniel Saraga

design: blaise Magnenat

Investigative journalist is essential for democracy.

How can it be protected from undue surveillance?

Investigative journalism is a crucial component of democracy. It keeps tabs on the activities of the most powerful actors in society, from governments to multinationals and very rich individuals. But both journalists and their sources are subject to political pressure and can face prosecution or even violence. While digital tools are helping collaborations of journalists worldwide, they also increase the chances that surveillance uncover their work. This is why the digital protection of journalist and sources is increasingly important.

Large media outlets such as The Guardian or The Washington Post are offering tools to communicate tips securely. The International Consortium of Investigative Journalists has developed with scientists a new system to help journalists share their document in a secure fashion. EPFL's Carmela Troncoso and Pierre Romera from the ICIJ explain how they collaborated to preserve journalists' security.

Here is a short press review on investigative journalists and the dangers they are facing.

2021 Nobel Peace Prize honours journalists
Two journalists received the 2021 Nobel Peace Prize for their "efforts to safeguard freedom of expression, a precondition for democracy": Maria Ressa, founder of digital media company Rappler specialising in investigative journalism, and Dmitry Muratov, editor-in-chief of the independent newspaper Novaya Gazeta. Both are subject of intense pressure from the authorities or criminal organisations. In the Philippines, Maria Ressa had to face ten arrest warrants from the government in less than two years, for charges carrying a total maximum penalty of more than 100 years. In Russia, six of Novaya Gazeta's journalists have been killed, including Anna Politkovskaya.

Secret offshore accounts exposed, again
On 3 October 2021, dozens of media outlets started publishing details on offshore accounts of over 300 world leaders, business leaders and celebrities. This followed an 18-month analysis of 12 million documents made by more than 600 journalists of 146 media working within the International Consortium of Investigative Journalists (ICIJ). They collaborated on Datashare, a secure platform maintained by ICIJ to protect their identity and reduce the risk of pressure, prosecution and attacks.

OECD sets a 15% minimal tax rate for multinationals
Almost all the 140 member states of the OECD agreed on 8 October 2021 on a reform of the international tax system. It will allow taxes on profits from around 100 of the world's largest multinationals to be allocated to the countries where the companies operate and generate revenues.

Media halts operation in Russia
The Organized Crime and Corruption Reporting Project – an international investigative journalism network – has announced on 15 September 2021 that it would stop operating in Russia and collaborate with journalists outside the country. The move was made to "protect journalists amid the Kremlin's campaign against independent journalism". The Russian government had declared an increasing number of investigative media outlets as being "foreign agents", making them lose advertising revenues.

Journalists in danger
354 journalists are currently imprisoned and more than 60 are killed every year, according to Reporters Without Borders.

A lawsuit to prevent spying
Reporters Without Borders (RSF) Germany has filed a lawsuit on 5 November 2021 against German intelligence agencies to curtail their abilities to hack into journalists' digital communications and spy on their activities. A new law has given intelligence agencies the permission to use spyware to hack into smartphones and computers and record encrypted messages and calls via services like Signal, Telegram and WhatsApp. This new situation puts journalists as well as their sources in danger. In July 2021, the International Federation of Journalists had also condemned the use of the Pegasus spyware to target 180 journalists worldwide.

Informant enters prison
Mayflower Edwards, who had leaked confidential documents to BuzzFeed News while working at the U.S. Treasury Department, started her 6-month jail sentence in September 2021. She had sent in 2017 and 2018 over 2000 suspicious activity reports documenting financial transactions linked to the Russian involvement in the 2016 U.S. presidential election, after she had gone through official channels.

Julian Assange might be extradited
The British High Court ruled in favour of an appeal made by the U.S. government, which should allow for Julian's Assange extradition to the U.S. A previous decision ruled against it because of the suicide risks in a maximum security prison. The founder of Wikileaks will probably appeal. He had stayed in the Ecuadorian embassy in London for seven years to escape prosecution in Sweden for alleged sexual offenses and was arrested upon his exit in April 2019. He is since then in a British jail, waiting for a final decision on his extradition.

“Our priority is to ensure the safety of journalists and sources”

Pierre Romera CTO of the International Consortium of Investigative Journalists (ICIJ)

ICIJ © 2018

© Shutterstock

The International Consortium of Investigative Journalists (ICIJ) is known for the three largest information leaks in history: the Panama, Paradise and Pandora Papers, which uncovered countless international financial malpractices. The organisation’s CTO, Pierre Romera, explains how they enable collaboration between journalists while protecting them.

Have you replaced Wikileaks?
Our approaches are entirely different. Wikileaks publishes all the documents without going through the journalistic analysis which we do. They mostly share documents from the government, including military classified information, while ours usually come from private companies. These include details of many people who would be endangered if everything was published. We make sure we do not compromise them.

How do you proceed?
We first spend a lot of time checking the reliability of the sources and the authenticity of the documents. We then make sure that what we publish is legally sound and that we cannot be prosecuted. The amounts of documents are huge: the financial leaks known as the Panama, Paradise and Pandora Papers contain more than 10 million documents, each.
We collaborated with over 150 media organisations around the world to analyse the information and reconstruct financial streams. This means the millions of documents we provide must be accessible and searchable by journalists everywhere.

Why is the ICIJ getting involved in data security and online protection?
Our first priority is to ensure the safety of the journalists working with us and of the sources of the leaked documents. It’s a moral obligation. And, of course, they would not work with us anymore if it was not perceived as being safe.
It is also crucial that the analysis phase – which can last months – is made in secrecy. This prevents the risk of attempts by the governments, companies or powerful individuals to prevent publication by exerting pressure on journalists or launching prosecution against them while they are analysing the information and preparing their report. Any journalist can be harassed, even in our modern democracies.
No one outside the ICIJ should know about our ongoing investigations so that our media partners know they can rely on

the agreed embargo. The latter is very important as it gives journalists the time to carefully investigate, analyse the data and make all the necessary checks without fear of seeing another media outlet publish prematurely because of a prosecution. The coordinated publication of investigations at the same time has a powerful impact. A local power has less motivation to try to prevent the publication when the information is anyway available in many other media outlets.

What security measures have you put in place?
On the technical side, we require from all our partners to use encrypted communication: PGP protocols for emails and encrypted chats such as Signal. This ensures that the communication remains safe also after publication, as hacking properly encrypted messages is in practice almost impossible, even later on.
We have built a platform, called Datashare, which allows our partners to query our documents in a secure manner and helps them identify people and companies involved in tax evasion or financial fraud.

Wouldn't it be simpler for them to download the data locally?
We don't allow it for several reasons. First, our sources entrust us with the information and do not want to see it circulated. It's important for us to keep control over the original document and make sure there are no copies going around, possibly with changes which we are not aware of. Second, the risk of a leak of a dataset increases every time it is transferred. Finally, maintaining databases with several terabytes of documents is expensive: it costs us for example around 20 000 dollars to make the Pandora Papers searchable by our partners. We don't want to impose such a financial burden on the media outlets interested in collaborating.

Your partners analyse in a remote and collaborative manner millions of leaked documents. What technical challenges does it entail?
Our architecture must balance security and ease of access. We could build a system impossible to hack, but it would be too hard to use, especially for media outlets with less technical expertise. That said, we have created an API to allow the automation of data queries and analyses.

You are working with EPFL scientists on the project Datashare Network. What will it bring?
In short, it replicates our Datashare system on the computers of journalists who want to contribute, hence going from a centralised trove of information to a decentralised one. Journalists often find themselves documents that could interest their colleagues. With Datashare Network, they will be able to install a software on their computer that allows other ICIJ members to search their documents securely.

Has the ICIJ been victim of cyberattacks?
Not on the data but on our infrastructures, yes. Our website had several Denial-of-service attacks (where bots try to flood a server with connection requests to make it unavailable online), two of which succeeded and slowed down access to our platform. But of course, the information kept being published by our media partners.

Have journalists of the ICIJ network ever been imprisoned?
No. Some have been threatened, but none sued. We have not published confidential documents from the government, except some from the U.S. Department of the Treasury, so the risk of prosecution is less than in Wikileaks' case.

Are journalists aware enough of the importance of digital protection?
Not all of them. One of our missions is to sensibilize them and train them to use secure digital tools, such as encrypted communication, choosing safe passwords or working on secured platforms. Before the internet, journalists would often meet their sources in person, without the risks created by online tools. But now, even offline meetings are not 100% safe because it is incredibly difficult to let no single digital trace behind you: your phone has a GPS signal, your Tweets and pictures might be geolocalised, the calls you make are tracked by relay antennas.... The largest media houses we work with, such as the Washington Post or The Guardian, are very much aware of these issues and support our efforts and measures.

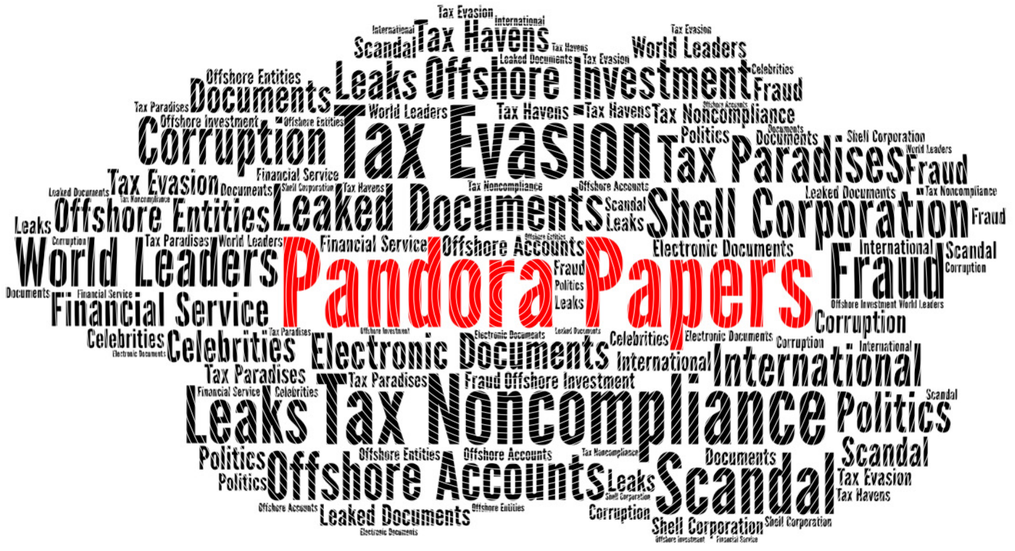
Is there a North/South divide in terms of access to technology, risk awareness and benefits sharing?
Yes, there is an imbalance. Some partners do not have access to good IT infrastructure: the internet connections

are slow or unstable, or their computers are not powerful enough to run complex analyses. We use two-factor authentication, but not every journalist owns a smartphone... And of course, data journalism is currently more known and practised in Western countries. But our consortium is built on internationality – half of our 150 media partners are outside Europe or North America – as well as solidarity: all the content produced by one newspaper, in particular the analyses, tables, charts and infographics, can be used by the partners. Often, the ICIJ produces them directly to facilitate sharing.

“You first have to look at all the possible weak points, starting with humans”

Carmela Troncoso Head of the Security and Privacy Engineering Laboratory at EPFL

C4DT FOCUS N°2 EPFL



Carmela Troncoso’s team at EPFL has developed a tool to help journalists share leaked documents securely. Made in collaboration with the International Consortium of Investigative Journalists, DataShare Network is even safe in case of a mole. Troncoso’s team is also known for their crucial contributions to the DP-3T protocol, used in privacy preserving contact tracing apps around the world.

How can specialists of digital security help journalists?
Digitalisation brings huge potential but also many risks, and mitigating them is where my team can help. Tax evasion, financial fraud and corruption cases are very connected. A journalist working on a story might focus only on companies in their country, disregarding the foreign businesses that appear in their document. But this information could interest other journalists working abroad, so sharing documents can help international investigations.
Before, journalists would mainly work with physical documents and use their informal network to find additional relevant information. Digitalisation makes it easier for them to share files and communicate rapidly with many colleagues around the world. And when organisations like the International Consortium of Investigative Journalists (ICIJ) make available the leaked documents they receive, more efficient searches are possible, enabling a new scale in investigative journalism.

But there is a big catch. Communications, especially on the internet, can be monitored and journalists and their sources have a greater risk of prosecution, imprisonment or violence.

Your team partnered with the ICIJ to improve their document sharing platform. How does it work?
The current system is called Datashare. It starts by scanning documents (pdfs, emails, spreadsheets) to extract three types of information: the organisations, locations and names of people mentioned in each file. It is this information – and not the document itself – that can be searched by the users on the platform. If there is a match, the user can view the file and download it. Importantly, this platform is centralised as it only share the documents in ICIJ’s possession. Journalist who themselves get access to other interesting documents cannot readily share them.

And the new project?
Our software, called Datashare Network allows any journalist accredited by the ICIJ to make their own document collections searchable by other members, by running the software locally. This obviously empowers even wider investigations. But you have to make sure it does not generate too many risks for the users.
What are the concrete dangers?
The journalists’ identities, the documents they have as well as

the kind of their queries they send must be protected to avoid risks of threats. The government, the security forces or the private companies they are researching should be not aware that an investigation is going on or, of course, be able to identify who is taking part in it. But digital messages sent by a journalist containing specific names or terms might get picked up by surveillance and alert third parties about an investigation. Once received, the messages are stored on other people's computers, which might be seized during a police operation, endangering many other users on the network.

How did you mitigate the risks?
You first have to look at all the possible weak points, starting with humans. In principle, one can trust the ICIJ and the journalists it accredited, and nobody else. But actually, it could happen that a journalist is coerced and turned into a mole asked to spy on the network. If a criminal or security personnel puts a gun on your head and tells you to get into the system, you'll probably do it. Our system ensures that users get as little information as possible in order to protect everyone on the network.
Technically, we encrypt both the queries and the documents' tags (people, organisations and locations) with advanced cryptographic techniques, in particular a novel form of Private Set Intersection, to verify if a query gets a hit. In this case, the querier will only know there was a hit, but not who has the document.

And they will see the document matching their query?
No, it would be a bad idea to display documents automatically. It would be like keeping your office open to everyone wanting to photocopy your files, and without you knowing about it. Hence, a second stage starts on Datashare Network: The querier and the user who owns the matched document can anonymously communicate via an encrypted single-use chat room, where they discuss the case and vet each other. This step is important, as journalists want to decide to whom they pass their information, because they might refuse to collaborate with people they don't trust or with a competing media. Once they agree, they exchange documents outside Datashare Network, for instance by using PGP email, a secure drop or sending an encrypted USB stick by the post.
To avoid leaving any digital traces of the communication, we create artificial fake, dummy traffic to obfuscate the queries and the chat rooms. There are additional security measures. Users must use a Tor network in order to avoid revealing IP addresses. Queries are sent together with a one-use token that proves the querier is a member from the ICIJ. This prevents the risk of bots sending millions of queries and siphoning out information from the system.

Comes the security at the expense of usability?
Yes. Our dummy traffic uses more bandwidth, which really is a limiting factor for journalists in developing countries. It's always bandwidth they care about. We interviewed 30 journalists to understand what balance between usability and security they need. To make the risks more tangible, we used a mock-up of the system where an adversary gets access to a laptop to show them what they would be able to learn, depending on the implemented security mechanisms.

How was the collaboration with the ICIJ?
It was smooth and active. We followed a co-design approach all along the project, with weekly Sprint meetings involving the IT teams of ICIJ. We first worked together for a year making sure we understood the requirements and concrete use cases to make sure our solution could be useful. We really do not want to be elitist academics who create perfect, but useless solutions!

Would it be also possible to collaborate securely in the further analysis of the documents, such as for data journalism?
We started discussing such a project with data journalists in Switzerland, but got halted by our work on the Covid app. Hopefully we can restart soon. But our capacity is limited, and so many NGOs have asked us for support on digital security issues.

© Shutterstock