UNESCO report: surveillance and data collection are putting journalists and sources at risk

Julie N. Posetti
University of Wollongong, jposetti@uow.edu.au

Publication Details
UNESCO report: surveillance and data collection are putting journalists and sources at risk

Abstract
Released this week, my UNESCO report Protecting Journalism Sources in the Digital Age shows that laws protecting journalists and sources globally are not keeping up with the challenges posed by indiscriminate data collection and the spill-over effects of anti-terrorism and national security legislation.

Keywords
unesco, report:, surveillance, data, collection, sources, putting, risk, journalists

Publication Details

This journal article is available at Research Online: http://ro.uow.edu.au/lhapapers/2960
Press freedom is being undermined by the global trend towards mass surveillance and data retention. www.shutterstock.com

UNESCO report: surveillance and data collection are putting journalists and sources at risk

May 3, 2017 3.54pm AEST

www.shutterstock.com

UNESCO report: surveillance and data collection are putting journalists and sources at risk

The ability of journalists to report without fear is under threat from mass surveillance and data retention.

1 of 5 4/5/17, 10:29 am
Released this week, my UNESCO report Protecting Journalism Sources in the Digital Age shows that laws protecting journalists and sources globally are not keeping up with the challenges posed by indiscriminate data collection and the spill-over effects of anti-terrorism and national security legislation.

Examining legal changes to how sources are protected across 121 countries between 2007-2015, I found that calls, text messages, and emails made in the process of reporting are increasingly exposed. In particular, they can be caught up in the nets of law enforcement and national security agencies as they trawl for evidence of criminal activity and terrorism, and conduct leak investigations.

Source protection laws should be updated to protect the online communications of journalists and whistleblowers.

If we do not strengthen legal protections and limit the impact of surveillance and data retention, investigative journalism that relies on confidential sources will be difficult to sustain.

**New technologies, new problems**

Now that simply using mobile technology, email, and social networks may result in a person being caught up in state and corporate surveillance and data mining, the laws protecting sources and journalists are being seriously undermined.

The study found that source protection laws globally are at risk of being:

- trumped by national security and anti-terrorism legislation that increasingly broadens definitions of “classified information” and limits exceptions for journalistic acts
- undercut by surveillance – both mass and targeted
- jeopardised by mandatory data retention policies and pressure applied to third party intermediaries to release data which risks exposing sources
- outdated when it comes to regulating the collection and use of digital data, such as whether information recorded without consent is admissible in a court case against either a journalist or a source; and whether digitally stored material gathered by journalistic actors is covered by existing source protection laws, and
- challenged by questions about entitlement to claim protection - as underscored by the questions: “Who is a journalist?” and “What is journalism?”

These threats suggest lawmakers need to think differently when it comes to protecting press freedoms.
In the past, the main concerns of courts and lawmakers was whether a journalist could be legally forced to reveal the confidential source of published information or be the subject of targeted surveillance and search and seizure operations.

Now that data is routinely intercepted and collected, we must find new ways to protect the right of journalists to withhold the identity of their sources.

The Australian metadata threat

Australia’s experience with mandatory metadata collection shows how complicated the question of journalist-source protection can become in a digital era.

The Australian Federal Police recently admitted to illegally accessing an unidentified journalist’s metadata without a warrant.

This breach was possible because of the country’s mandatory data retention law, which requires phone and internet companies to preserve user metadata for two years, even when there is no suspicion of a crime. This includes information such as when a text message was sent and who received it, but not its content.

Advocates of long-term metadata retention, like Australian Attorney General George Brandis, have insisted the law poses no significant threat to privacy or freedom of expression. When the legislation was enacted in March 2015, it included an amendment that requires government agencies to seek a warrant to access journalists’ communications with sources in certain cases.

UNESCO report: surveillance and data collection are putting journalists and sources at risk https://theconversation.com/unesco-report-surveillance-and-data-collection-are-putting-journalists-an...
Transparency, however, is not required. Revelation of the existence (or non-existence) of such a warrant is punishable by a two-year jail term. At no point are journalists nor media organisations advised of such an intervention, and there is no opportunity for them to challenge the issuing of a warrant.

These shortcomings mean the law fails seven out of 11 indicators in UNESCO’s guide for measuring the effectiveness of a country’s legal source protection framework.

In the face of these threats, journalists can take steps to protect their online security and ensure sources have ways to contact them securely. Yet even when they encrypt the content of their source communications, they may neglect the metadata, meaning they still leave behind a digital trail of whom they contacted. This data can easily identify a source, and safeguards against its illegitimate use are frequently limited or non-existent.

Australia’s Press Council chair, professor David Weisbrot has said mandatory data retention legislation risks “crushing” investigative journalism:

> I think that whistleblowers who are inside governments or corporations will definitely not come forward because their confidentiality and anonymity will not be guaranteed. If they came forward, a journalist would have to say ‘I have to give you some elaborate instructions to avoid detection: don’t drive to our meeting, don’t carry your cell phone, don’t put this on your computer, handwrite whatever you’re going to give me’.

Australia’s metadata experience shows how legal protections that shield journalists from disclosing confidential sources may be undercut by backdoor access to data.

This also applies to information collected by internet service providers, search engines, and social media platforms. Such companies can, in some circumstances, be compelled by law enforcement to produce electronic records that identify journalists’ sources.

In an interview for the UNESCO study, Privacy International legal officer Tomaso Falchetta said

> There is a growing trend of delegation by law enforcement of quasi-judicial responsibilities to Internet and telecommunication companies, including by requiring them to incorporate vulnerabilities in their networks to ensure that they are ‘wire-tap ready’

On World Press Freedom Day, we’d like a little less secrecy, and lot more accountability.
UNESCO report: surveillance and data collection are putting journalists and sources at risk

https://theconversation.com/unesco-report-surveillance-and-data-collection-are-putting-journalists-an...