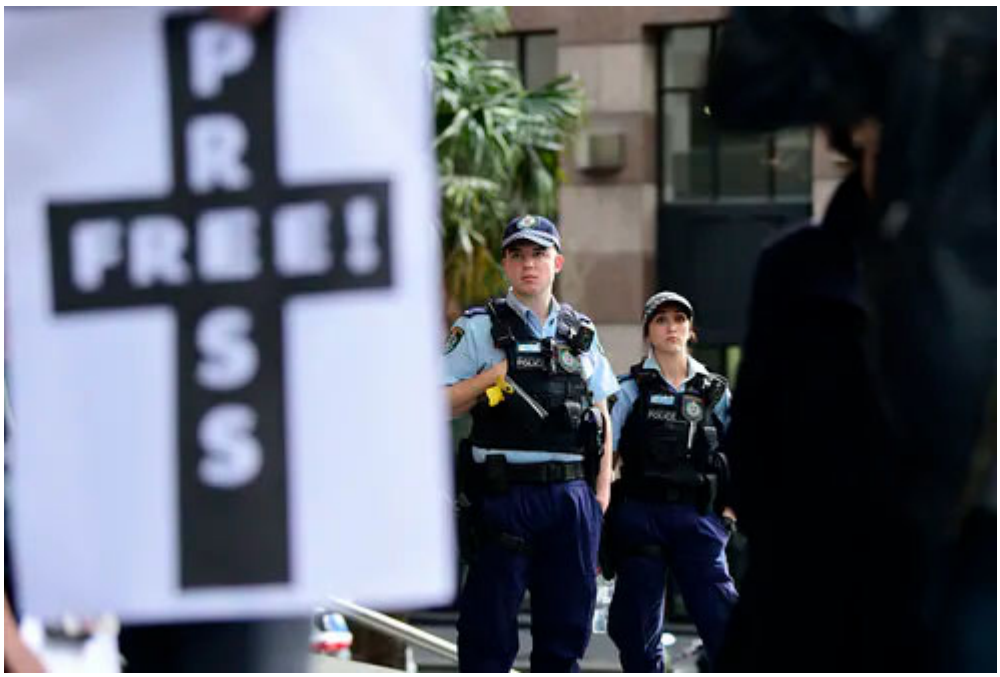
THE CONVERSATION
Academic rigour, journalistic flair



Metadata access has serious implications for Australia's diminishing press freedom and whistleblower protections. AAP Image/Bianca De Marchi

Unlawful metadata access is easy when we're flogging a dead law

December 10, 2019 1.25pm AEDT

After watching this year's media raids and the prosecution of lawyers and whistleblowers, it's not hard to see why Australians wonder about excessive police power and dwindling journalistic freedom.

But these problems are compounded by another, less known issue: police, and other bodies not even involved in law enforcement, have broad powers to access metadata. Each year, police alone access metadata in excess of 300,000 times.

Metadata has been described as an "activity log": it's the information that allows a communication to occur. Once, this would have been the address on the envelope. But modern telecommunications metadata consists of the time, date, duration, locations of a connection and more.

Authors

Genna Churches
PhD Candidate, UNSW

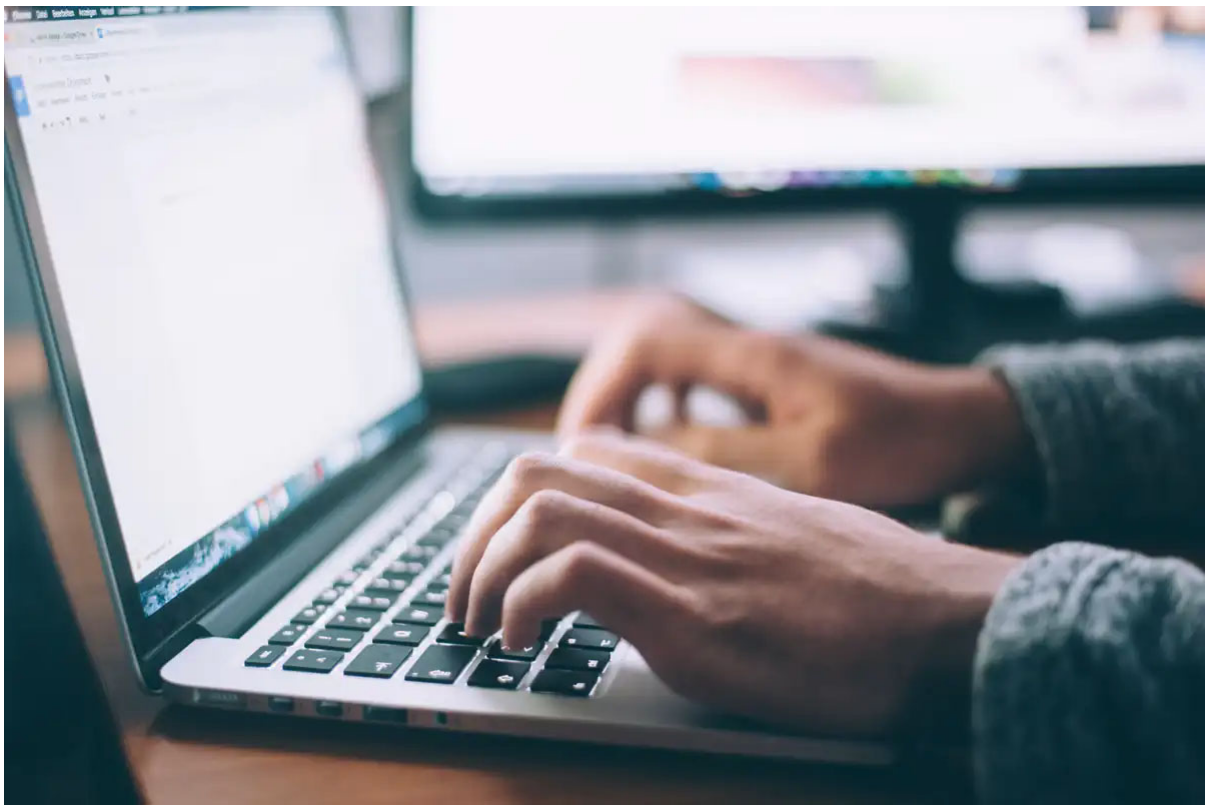
Monika Zalnieriute
Research Fellow, Lead of 'Technologies and Rule of Law' Stream, UNSW

Read more: Infographic: Metadata and data retention explained

This year, fresh evidence revealed police accessed the metadata of journalists and 3,365 telecommunications users unlawfully.

And local governments and professional bodies – which were explicitly denied access to metadata in 2015 – have been accessing the same data under different legislation.

What's more, Optus this year revealed it was granted an exemption from a requirement to encrypt retained metadata. This means the metadata they hold isn't secure.



Metadata can reveal where you work, live, who you visit, who you communicate with. Glenn Carstens Peters/Unsplash

So why are so many agencies overstepping their powers? The obvious answer is, of course, because they can.

There's little oversight and consistency in the current metadata regime. The system is spread across two separate pieces of legislation, enacted decades ago, with more than 100 amendments.

This leaves loopholes that various agencies and police exploit for accessing metadata and dodging safeguards.

Why should I care about metadata anyway?

These scandals surrounding the metadata regime have cast a shadow over the Parliamentary Joint Committee on Intelligence and Security's current review of the outdated laws.

Read more: Think your metadata is only visible to national security agencies? Think again

---

Metadata can reveal where you work, live, who you visit, who you communicate with and potentially reveal your plans by exposing websites you access.

Australian law considers metadata less important than "content" (the voice in a live phone call or message in an email).

So while intercepting a phone call or email requires a warrant, metadata is accessible without a warrant by law enforcement agencies and any other bodies the legislation authorises, such as local governments.

The Abbott-era metadata scheme limits press freedom

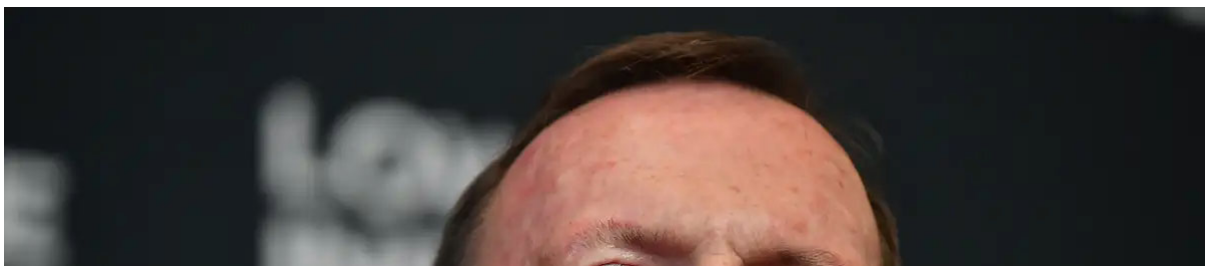
In 2015, federal parliament, as part of efforts to target terrorism, passed the metadata retention scheme used today, requiring telcos to keep metadata for two years.

Read more: Benign and powerful: the contradictory language of metadata retention

---

Attempting to address privacy concerns, parliament limited the types of organisations that could access the data and the specific types of metadata that could be retained (excluding web browsing histories). It also created "journalists information warrants" to protect journalists' sources.

Despite evidence suggesting these limitations wouldn't work in practice, the legislation was passed.



Tony Abbott's government brought in the ineffective metadata retention scheme that's still used today. AAP Image/Joel Carrett

It committed Australia to a data retention scheme at a time when a similar scheme in Europe was ruled invalid for being incompatible with fundamental rights.

Confusing laws mean safeguards don't work

Law enforcement and intelligence agencies should have access to metadata, but the current system does not strike the right balance between privacy and law enforcement.

The gaps between the two laws that regulate the scheme allow the agencies and police to exploit them for their own purposes.

The first act, originally enacted in 1979 and amended at least 105 times over the last 40 years, was originally drafted to permit telephone intercepts.

The second act, Telecommunications Act 1997 originally contained provisions permitting access to metadata. But some elements were transferred to the 1979 act, leaving a broken and contradictory system of access and loopholes spread across the legislation.

Read more: Australian metadata laws put confidential interviews at risk, with no protections for research

---

These "logistical" issues result in a metadata access and retention scheme with very few safeguards.

Other safeguards are flawed: access to a journalist's metadata under a "journalist information warrant" doesn't actually protect sources, especially since the Public Interest Advocate isn't bound to make a submission.

And others were deemed unnecessary, like restrictions on access to a lawyer's metadata, despite professional secrecy obligations; or a requirement beyond a "self-authorisation" to access metadata in general.

So, what should we do to fix the Australian system?

Put simply, Australian communications have changed, so our metadata access laws need to change too. We can start by recognising modern metadata retention and access has large scale privacy implications, surpassing those surrounding telephone intercepts.

We need to assess those implications based on what metadata – now collected and processed via very different technologies – can reveal.

Accessing particularly sensitive types of metadata should require a judicial warrant and an investigation of a sufficiently serious offence that leads to imprisonment.

On the other hand, access to subscriber details, such as name and address, may be available under a less rigorous system of access, but still must be more restricted than the current regime. Even name and address information can be open to abuse.

Read more: Explainer: how law enforcement decodes your photos

---

Past parliamentary inquiries and reviews held throughout 2000s and 2010s have recommended a complete reform of the metadata regime. But these calls have gone unanswered.

We hope the current review also recommends a complete overhaul. A new review to redesign the scheme should be commissioned as soon as possible.

Above all, the government should consider the impact of such system on human rights. Australians deserve to know that access to their metadata is limited, and that metadata access will not be used to prosecute whistle-blowers and journalists for doing their jobs.

Metadata **Legislation**