THE CONVERSATION
Academic rigour, journalistic flair

Who watches the watchers when the watchers use Wickr?

October 9, 2015 4.12pm AEDT

Malcolm Turnbull is known to use secretive messaging apps such as Wickr. AAP Image/Lukas Coch

Author

Bruce Baer Arnold
Assistant Professor, School of Law, University of Canberra

The latest controversy over Malcolm Turnbull's use of Wickr should provoke questions about accountability in the age of the cloud.

It's an age where use of private messaging systems by a digital 1% – an elite that is well connected and powerful – is eroding expectations about oversight by journalists, official monitors and ordinary people. To adapt the words of writer David Brin, a privileged "Them" know a lot about us and increasingly "We" know less about them.

Governments have always sought to keep some communications secret, whether by using technologies (everything from special couriers to encrypted fax, email and voice communications) or by relying on face to face meetings and "old boys" networks.

In doing so, they're like the private sector, but with greater resources than most Australian enterprises. Understandably, Australia's national government has not published a blueprint of which tools, such as Wickr, are being used by parliamentarians, officials, members of special inquiries and others who deal with information that is politically sensitive or official.

People who are aware of how the tools are being used are typically reticent about disclosing specifics, whether because of a sense of responsibility or because of secrecy provisions regarding particular agencies.

One implication is that we need to trust that the government knows what it is doing, i.e. it has been properly advised by experts in bodies such as the Australian Signals Directorate about what's secure and what isn't.

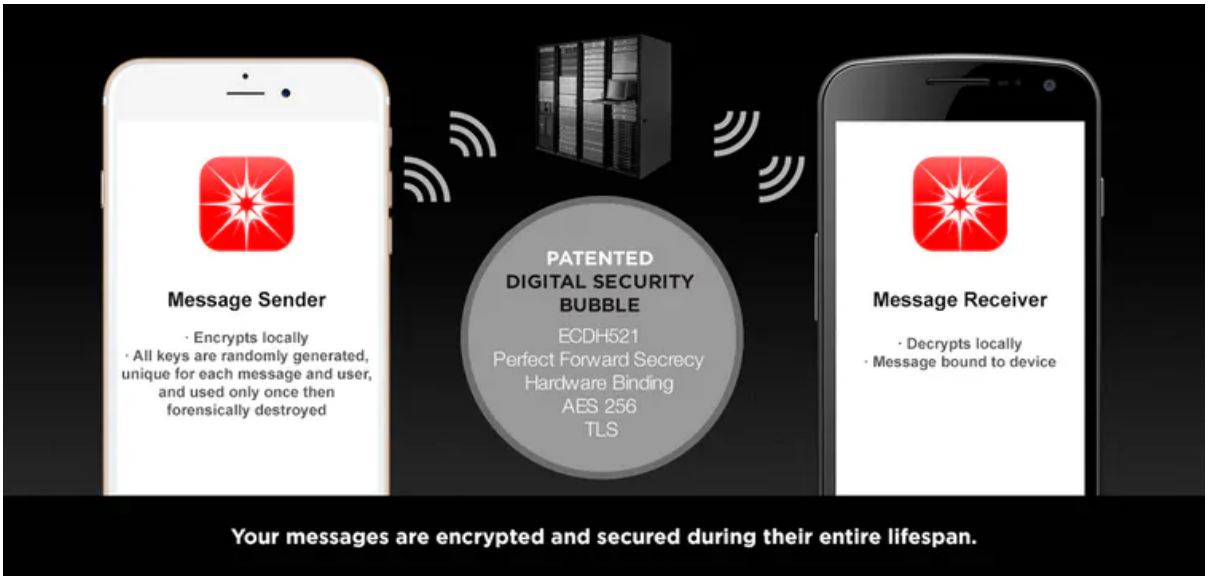
Freedom from information

Another implication is uncertainty about accountability.

Ministers and public sector agencies are distinguished from the private sector because they are meant to be accountable. That accountability is broader than the Freedom of Information and Archives legislation, which are aimed at ensuring citizen access to government information.

Accountability is enshrined in judgements by Australian Courts recognising that knowing what the government is doing is the foundation of the liberal democratic state. A salient example is the statement by Justice Michael McHugh in the Spycatcher Case (where Turnbull was a barrister) about responsibility.

In principle, use of tools such as Wickr for official communications by ministers, other MPs and officials is directly covered by the FOI Act (access to contemporary communications) and the Archives Act (historic material).



Wickr offers private communication between two parties, unlike SMS. Wickr

Those enactments feature broad exemptions that reflect legitimate concerns regarding personal privacy, commercial confidentiality and national security. Only utopians, such as Julian Assange, who want the state to evaporate would want total transparency.

Who's watching?

In practice the use of external – essentially private – services and devices has a fundamental impact on the FOI and Archives regime. Irrespective of whether you are an archivist, a journalist, a potential litigant or another MP, you are very unlikely to access and preserve a communication if you have no way of determining whether that communication has taken place.

You cannot rely on the Office of the Australian Information Commissioner (OAIC's), the complacent agency that has been grossly underfunded and has undergone regulatory capture.

The government remains committed to abolishing that watchdog, irrespective of the OAIC's lack of vigour and recalcitrance about FOI applications regarding that agency's own operation.

The Prime Minister has not condemned recurrent statements by Public Service Commissioner John Lloyd that FOI is "pernicious" and has gone too far, a signal from the top that bureaucratic convenience is far more important than accountability.

The National Archives, still alive but seriously underfunded, faces the same challenges as its oversees peers in preserving electronic records, i.e. the email, Microsoft Office and other documents that are "born digital", are readily deleted and are less robust than paper.

If the organisation is struggling with mundane email, it's not going to cope well with messaging systems based on encryption, and which users claim involve private communication. A diligent scholar can identify the archiving protocols for email within many government agencies. Don't be optimistic about voice calls, particularly calls by an important "Them" using services that promoted as sidestepping the archivist or FOI applicant.

Freedom from oversight

Wickr-style services will grow. In thinking about government use we should recall that the Trans-Pacific Partnership Agreement – the details of which are still secret – appears likely to prevent Australia from prohibiting offshoring of data and thus limiting the cloud.

We should also recall that neither the government nor opposition has resiled from warrantless access by a wide range of agencies to whole-of-population telecommunications metadata that is mandatorily retained by telecommunications companies.

We might be optimistic, and decide that leaks within and around Cabinet will provide us with everything we need to know, irrespective of whether a meeting takes place at the Melbourne Club or someone used Wickr.

However, a realist might wonder whether such tools mean that "free speech" is a privilege of a digital 1%, those rare people who are free not to be observed, and whether ministers should be reminded that FOI does not mean unaccountability through a freedom from oversight.

Cloud computing **Digital privacy** **Malcolm Turnbull** **Freedom of information** **SMS** **Digital records** **Freedom of Information Act**