# Data retention flopped in Europe and should be rejected here

August 7 2014, by Bruce Baer Arnold

The Coalition's data retention plan, if implemented, will cause headaches for the government, businesses and users. Credit: Hector Parayuelos/Flickr, CC BY-NC-ND

When it comes to metadata the federal government appears to have learnt nothing and forgotten everything. Statements this week by Prime Minister Tony Abbott and Attorney-General George Brandis display the same confusion evident in recent testimony to parliament by the head of ASIO, David Irvine.

Are we going to have mandatory metadata retention, and for how long? Warrantless access to data about every phone call, SMS, tweet and web session? Access by local government rather than just by ASIO and the police?

We can learn from experience in Europe, where courts and data protection agencies have rejected mandatory retention of bulk metadata. We should also heed cautions in the US, where a range of experts have warned that metadata is not a surefire way to prevent terrorism and what our Prime Minister characterises as "general crime".

The national government is proposing mandatory retention by telecommunication providers and other businesses of data about the electronic communications of all Australians. The data would be held by those enterprises, with access being given to a range of public and private sector entities.

The Prime Minister's office yesterday confirmed access to "content", such as web browsing history, will require a warrant, but it appears that access to metadata will be given without a warrant, a fundamental erosion of accountability but very convenient for law enforcement and national security agencies.

## The view abroad

Mandatory retention – a requirement by national law that businesses store data – has been promoted by the Council of Europe under the global Cybercrime Convention. Australia is a member of that agreement, and for more than a decade there have been calls by Australian police and other agencies that our telcos, internet service providers (ISPs) and social network services must keep metadata for a period of two, five, seven or 10 years. (The two-year period in the current proposal is arbitrary.)

Businesses store the data at their own expense, so it is a regulatory cost. In Europe, businesses indicated that they didn't want to bear the storage cost and administer diverse requests for access to that data, and they did not want to restructure their systems to keep track of billions of SMS and records of web surfing.

Those costs aren't trivial – Australia's second-largest ISP iiNet estimated it would cost A$60 million just to build a suitable storage facility.

Furore in Europe saw critics worry that data would leak, fostering identity offences. In Australia it is worth recalling recurrent large-scale data breaches involving our leading phone companies, departments and other "best practice" organisations, so the danger isn't entirely far-fetched.

Just as importantly, mandatory retention is disproportionate. European courts have damned the retention as significantly eroding respect for privacy under national and EU-wide law. In a liberal democratic state it is axiomatic that not everyone be considered a "suspect", a potential criminal whose life can be tracked via their electronic presence over a period of several years.

The courts were unpersuaded that long-term retention of data about whole populations was effective. Their scepticism was reinforced by the availability under EU law of requirements to collect, maintain and provide data about particular individuals and numbers.

Contrary to hyperbole by the Assistant Commissioner of the Australian Federal Police in 2012, law enforcement in Europe hasn't ceased. There's been broad community support for activity that is both *lawful* and *proportionate*. But proportionate is not the same as bureaucratically convenient, a point apparently missed by our sadly confused Attorney-General but recognised by Greens Senator Scott Ludlam in his

questioning of the ASIO Director-General.

## Where's the trust?

Sadly, if Brandis cannot provide a coherent explanation of what he is trying to do we cannot trust him, and trust is fundamental to the proposal gaining support.

We should not all be regarded as suspects of terrorism or a meaninglessly broad category of "general crime". We should not be subject to the chill associated with knowing that the police – and other entities – will be able to identify who we called, who read our tweets, when we called, where we were located, whether we visited Facebook and who read our posts. The data should not be provided without a warrant.

Like Europe, we should reject ill-considered bureaucratic over-reaching and instead seek to strengthen privacy law and reinforce the legitimacy of the national security regime by better equipping bodies such as the Inspector General of Intelligence and Security (IGIS).

*This story is published courtesy of* The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation

Citation: Data retention flopped in Europe and should be rejected here (2014, August 7) retrieved 27 April 2024 from https://phys.org/news/2014-08-retention-flopped-europe.html