Data retention: Whatever Washington Wants, Nicola Does!

by staff report via fancy - SMH *Monday, Sep 3 2012, 12:47pm*
international / prose / post

Australia is SOVEREIGN, girls, try and remember!

> Between the two of them -- Gillard and Roxon -- the only thing Australian left in the room is a CRINGE! Wake up girls, you really do have minds and the ability to think for yourselves or did Rudd get it right when he blurted that after winning government 'we won't have to do anything' [of our own accord!]

Bimbo Attorney General, Nicola Roxon

It really is getting boring and tedious watching Canberra pollies kowtow to Washington's every whim and dictate -- FIVE military bases anyone?

[Strategically] well placed small nations have an edge on superpowers, they can play all sides off against each other to huge advantage, but of course a modicum of political nous is required and unfortunately, as we read below no serving government minister is able to think for themselves let alone ACT in Australia's best interests. Careful girls, you might join Howard and his boys in the dock for treason -- we're an equal opportunity judiciary in Oz.

Story from the SMH follows:

> **Roxon snaps to attention on online data retention**
>
> Attorney-General Nicola Roxon appears to have swung her support behind a controversial plan to capture the online data of all Australians, despite only six weeks ago saying ''the case had yet to be made'' for the policy.
>
> The data retention plan - which would force all Australian telcos and internet service providers to store the online data of all Australians for up to two years - is the most controversial element of a package of more than 40 proposed changes to national security legislation.
>
> If passed, the proposals would be the most significant expansion of national security powers since the Howard-era reforms of the early 2000s.

In a speech to be delivered at the Security in Government conference in Canberra today, Ms Roxon will say that law enforcement agencies need the data retention policy in order to be able to effectively target criminals.

''Many investigations require law enforcement to build a picture of criminal activity over a period of time. Without data retention, this capability will be lost,'' she will say, in a draft of the speech provided to Fairfax Media yesterday.

She will also say technological advancement since the advent of the internet is providing increasing room to hide for criminals and those who threaten Australia's security.

''The intention behind the proposed reform is to allow law enforcement agencies to continue investigating crime in light of new technologies. The loss of this capability would be a major blow to our law enforcement agencies and to Australia's national security."

But in an interview with Fairfax Media in mid July, Ms Roxon appeared to have a different view. ''I'm not yet convinced that the cost and the return - the cost both to industry and the [privacy] cost to individuals - that we've made the case for what it is that people use in a way that benefits our national security,'' she said.

''I think there is a genuine question to be tested, which is why it's such a big part of the proposal.''

Her apparent change of mind may be a result of conversations with the Australian Federal Police, who have long pushed for mandatory online data retention. Neil Gaughan heads the AFP's High Tech Crime Centre and is a vocal advocate for the policy.

''Without data retention laws I can guarantee you that the AFP won't be able to investigate groups such as Anonymous over data breaches because we won't be able to enforce the law,'' he told a cyber security conference recently.

But Andrew Lewman, the executive director of the Tor software project, which disguises a person's location when surfing the web, challenges that view. In July he told Fairfax Media data retention impedes the effectiveness of law enforcement.

''It sounds good and something sexy that politicians should get behind. However, it doesn't stop crime, it builds a massive dossier on everyone at millisecond resolution, and creates more work and challenges for law enforcement to catch actual criminals.

''The problem isn't too little data, the problem is there is already too much data.''

Proposals 'characteristic of a police state'

The proposals are being examined by the Joint Parliamentary Committee on Intelligence and Security to provide partial scrutiny of Australia's intelligence community.

The committee has thus far received almost 200 submissions from the agencies, members of the public as well as civil liberties and online rights groups.

In a heated submission to the inquiry, Victoria's Acting Privacy Commissioner, Anthony

Bendall, dubbed the proposals ''characteristic of a police state'', arguing that data retention in particular was ''premised on the assumption that all citizens should be monitored''.

''Not only does this completely remove the presumption of innocence which all persons are afforded, it goes against one of the essential dimensions of human rights and privacy law: freedom from surveillance and arbitrary intrusions into a person's life."

ISP iiNet said government had failed to demonstrate how current laws were failing or how criminals and terrorists posed a threat to networks, and said asking carriers to intercept and store customers' data for two years could make them ''agents of the state'' and increase costs.

A joint submission from telco industry groups argued it would cost between $500 million and $700 million to keep data for two years. It called for full compensation from the government's security agencies.

The Australian Federal Police and the Australian Taxation Office were among the few supporting the proposal to retain telecommunications data.

The ATO said the proposal would be consistent with European practices and that being able to access real-time telecommunications data would allow it to ''respond more effectively'' to attempts to defraud the Commonwealth.

The AFP, in its submission, said interception capabilities were increasingly being ''undermined'' by fundamental changes to the telecommunications industry and communications technologies. It said telco reform was needed "in order to avoid further degradation of existing capability".

Through the use of case studies, the AFP argued that on numerous occasions it had been restricted by what it could do under current telecommunications laws, and said that many offences went un-prosecuted because of this.

Costs may be passed on to consumers

The AFP conceded that the volume of data and its retention by telcos for use as evidence for agencies presented "challenges", but didn’t disclose how such challenges could be tackled.

Such challenges were highlighted in submissions by others like Victoria's Acting Privacy Commissioner Anthony Bendall. He said smaller ISPs, for instance, "may not be able to afford the data storage costs, and these costs may be passed on to consumers".

"It would appear that public support for this type of proposal is largely absent," Bendall said.

Users may abandon web

Bendall also said that data retention could "create an extreme chilling effect" not only on technology but on social interactions, many of which are now conducted solely online.

"Users may move away from using online services due to the fear that their communications are being monitored," he said. "Simply put, the proposal could mean that individuals, due to concerns about surveillance, revert back to offline transactions.

"If this occurred, it would affect existing efficiencies of both businesses and government," he said.

The Australian Privacy Foundation was just as scathing.

"Too many of the proposals outlined ... would herald a major and unacceptable increase in the powers of law enforcement and national security agencies to intrude into the lives of all Australians," the APF said.

The APF said the discussion paper released with the proposals was "misleading, and probably intentionally so".

Fears for journalist's sources

It's not just privacy advocates and telcos that expressed concern with the proposals, but the journalist union, the Media Entertainment and Arts Alliance. In its submission it said it was concerned that any expansion of interception powers and the powers of intelligence agencies had "the potential to threaten press freedom".

"There is considerable concern about the power of police and intelligence agencies to intercept communications, a concern not given proper consideration in the terms of reference," the MEAA said.

Online users' lobby group Electronics Frontiers Australia raised similar concerns to others but pointed out that one of the 40 proposed changes to national security legislation, which required people to divulge passwords, could lead to self-incrimination. It said should such a law be enacted it would undermine "the right of individuals to not co-operate with an investigation".

The lobby group also highlighted concerns with another proposal which would allow the Australian Security Intelligence Organisation to use an innocent person's computer to get into a suspect's computer. "The proposal that ASIO would be permitted to 'add, delete or alter data or interfere with, interrupt, or obstruct the lawful use of a computer' could lead to some very serious consequences," it said.

Such consequences could include, it said, pollution of evidence, potentially leading to failures of convictions. It could also provide the means for evidence to be "planted" on innocent parties, it said.

From ZDNet:

Australian customers could pay for govt spying
by Josh Taylor

ISP customers might have to pay for the privilege of having their internet browsing data stored for law-enforcement agencies if government plans go ahead, according to Optus.

If the Australian Government moves ahead with its plans to force internet service providers (ISPs) to retain customer data for two years just in case law-enforcement agencies need it, Optus has warned that the cost to set up these systems could be passed on to consumers.

As part of a review of national telecommunications legislation, the Australian Government has flagged that it may force ISPs to store as yet unspecified data for two years to assist police investigations.

David Epstein, the head of regulatory affairs at Australia's second-largest telecommunications company, Optus, told ZDNet that if the government moves ahead with these proposals and doesn't share the cost for building infrastructure to collect and store the data, this could be passed on to customers.

"Someone has to bear the costs of all of these things. The more detailed they are, the more expensive they are. It's not just a simple cost that can be absorbed," he said. "To do these things to the degree some people want to do them is a very, very costly exercise requiring massive storage capacity, let alone the ability to filter the information itself."

Epstein's comments were reflected in industry submissions to the proposal. The Communications Alliance estimated that the cost of data retention could be in the range of "tens to hundreds of millions of dollars" and if source and destination IP addresses are required to be included, setting up technology to capture this information would cost between AU$500 million and AU$700 million. The addition of a single data element could increase this figure by tens of millions of dollars.

Although Attorney-General Nicola Roxon was initially hesitant about the data-retention component of the review, in a speech to the Security in Government conference in Canberra this morning, Roxon showed that she has warmed to the proposal, stating that data retention is critical for law enforcement to do its job.

"Many investigations require law enforcement to build a picture of criminal activity over a period of time. Without data retention, this capability will be lost," she said.

"The intention behind the proposed reform is to allow law-enforcement agencies to continue investigating crime in light of new technologies. The loss of this capability would be a major blow to our law-enforcement agencies and to Australia's national security."

Although Roxon said that the government would take onboard the public discussion surrounding the proposals, her speech indicated that the government appears to be intent on bringing in data-retention legislation.

"We cannot live in a society where criminals and terrorists operate freely on the internet without fear of prosecution. We cannot allow technology to create a 'safe haven' for criminals, or a 'no-go' zone for law enforcement," she said.

"But this does not mean unfettered access to private data, either. What it does mean are carefully drafted, tested, and oversighted national security laws — and this is what I'm focused on delivering."

At a press conference after the event, Roxon told journalists that she didn't believe consumers would

be forced to pay in order for telecommunications companies to adapt to the changes.

"It's something that's now part of doing business in a changing technological world. And we are very open in our discussions with the industry about what will be a normal part of their business, what the legal framework will be, and we're taking seriously the issues that they're raising with us as well."

It is unclear whether legislation to enact data retention will be entered into parliament before the 2013 election. Roxon has reportedly delayed legislation until well after the parliamentary committee has reported back on the proposal, and the Cabinet will not consider any legislation proposals until May 2013.

The parliamentary committee conducting the review of the legislation will hold its first hearing tomorrow in Melbourne, with the Victorian Privacy Commissioner, Macquarie Telecom, South Australian and Victorian Police, and the Institute of Public Affairs all speaking.

http://tinyurl.com/bwhh9y2
