Australian Privacy Foundation

mail@privacy.org.au

http://www.privacy.org.au

MEDIA RELEASE

13 October 2015

Not Smart Online! – Data Retention launches Full of Holes

Despite the launch of mandatory two year data retention at midnight on October 13th, significant confusion remains within the telecommunications sector regarding exactly what is required to comply with the legislation. At a minimum, it is expected that providers will be required to retain

- IP addresses for each device or connection to the internet (including from computers, tablets, phones, etc)
- Time and duration of internet connections
- Volume of uploads and downloads
- Recipients of emails, along with date and time sent (Australian ISP emails only)
- Size of email attachments (Australian ISP emails only)
- Phone numbers called (even where the receiving party did not answer), on all landlines (including VoIP) and mobiles, along with the date and time of the call
- SMSs sent, along with the date and time of the SMS
- Rough location of user at time of call or SMS

Prime Minister Turnbull was similarly confused in his 2012 Alfred Deakin Lecture. According to the then Shadow Communications Minister, Mr Turnbull insisted that “while the purported intent is that only metadata – data about data – will be available to law enforcement, security and intelligence agencies, there is no explanation of how metadata will be distinguished from data (the two are often commingled, as in the ‘subject’ line of emails)”.

Though commenting at the time on data retention proposals being put forward by then Attorney General Nicola Roxon, Mr Turnbull’s comments apply equally well to the current data retention amendments passed by the current Coalition government with bipartisan support from Labor.

Mr Turnbull is of course a noted user of secret messaging app Wickr, which allows a user to send encrypted messages without trackable metadata. Mr Turnbull has also recently acknowledged that he and other members of parliament frequently make use of non-government email servers, raising serious concerns about government accountability at a time when the government is instituting an indiscriminate mass surveillance initiative that will be remarkably easy to circumvent. Private email providers such as Fastmail, for instance, have asserted that they are not classified as telecommunications carriers, and thus that they have an exclusion from mandatory data retention under the Over the Top provisions in the legislation.

Further risks posed by the mass collection and retention of telecommunications data include the potential for scope creep, including the use of such data in litigation unrelated to crime prevention and national security. As of October 13, a broad range of agencies will have access to this information without a warrant. The number of requesting agencies will likely expand in

future, as significant discretion is given to the Attorney-General in the mandatory data retention legislation to declare bodies or authorities to be a 'criminal law-enforcement agency' for the purposes of the data retention regime. In the absence of judicial oversight to access personal information stored by telecommunication providers, safeguarding bodies are reduced to conducting 'reviews' of the program that almost exclusively depends on an abuse already being discovered. One such reviewing body, The Office of the Australian Information Commissioner, is underfunded and still slated for abolition by the current government.

The federal government has allocated $131 million over 3 years to help telecommunications providers comply with the current mandatory data legislation; however the industry has warned that this will not be sufficient to cover costs. This means that costs will be passed on to consumers, and Australians will be left in the unenviable position of funding their own surveillance. In his critique of Labor's mandatory data retention policy in 2012, Mr Turnbull noted that there had not "…been an explanation of what costs and benefits have been estimated for this sweeping and intrusive new power, how these were arrived at, what (if any) cost was ascribed to its chilling effect on free speech, and whether any gains in national security or law enforcement asserted as justification for the changes will be monitored and verified should they be enacted." Since then, the Coalition have similarly failed to elaborate on these aspects of their own policy.

These costs come at a price of a mass surveillance regime that will have little to no impact on preventing organised crime and terrorism. In the United States, senior White House advisers and judges have raised questions about the ability of metadata retention to assist in preventing terrorist incidents, concluding there were "serious doubts about the efficacy of the metadata collection program as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism." The relative ease through which the laws can be circumvented, including by our current Prime Minister while performing the duties of Parliament, raises questions about the effectiveness of the initiative as a response to organised crime. The Australian Privacy Foundation also notes that similar mandatory data retention legislation has been invalidated in courts throughout Europe as a disproportionate risk to privacy and human rights.

The Australian Privacy Foundation is the primary association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions. It works with consumer organizations, civil liberties councils, professional associations and other community groups on specific privacy issues. The Privacy Foundation is also a participant in Privacy International, the world-wide privacy protection network.

The Australian Privacy Foundation's detailed submission to the PJCIS on mandatory data retention from earlier this year can be found at https://www.privacy.org.au/Papers/PJCIS-DataRetention-150119.pdf

Contacts for This Media Release:

*	Adam Molnar	Adam.Molnar@privacy.org.au	0499 993 412	@admmo
*	Angela Daly	Angela.Daly@privacy.org.au	(03) 9214 4420	@nidhalaigh
*	Liam Pomfret	Liam.Pomfret@privacy.org.au	(07) 3346 8170	@LiamPomfret
*	Roger Clarke	Roger.Clarke@privacy.org.au	(02) 6288 6916	