August 2018
Geoff Huston

The Law of Snooping

There is a saying, attributed to Abraham Maslow, that when all you have is a hammer then everything looks like a nail. A variation is that when all you have is a hammer, then all you can do it hit things! For a legislative body, when all you can do is enact legislation, then that's all you do! Even when it's pretty clear that the underlying issues do not appear to be all that amenable to legislative measures, some legislatures will boldly step forward into the uncertain morass and legislate where wiser heads may have taken a more cautious and considered stance.

We are talking about a proposed bill to be debated by the Australian Parliament. This is the "Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 No. , 2018 (Attorney-General) A Bill for an Act to amend the law relating to telecommunications, computer access warrants and search warrants, and for other purposes." So, it's all about telecommunications, right? Well no. It's actually about digital services. And it's not about telecommunications services per se. It's about services that are accessed via a telecommunications carriage service. Or services that could be accessed via a telecommunications carriage service. Or any other digital service!

Yes, it makes about as much sense as including regulations about housing in road legislation because, after all, you might use a public road to get to your house. But there is something more substantial going on here. It appears that within the Australian environment the digital services environment is not readily slotted into any existing conventional area of regulated activity. And in the past the telecommunications sector has been willingly compliant to various government demands for wiretap capabilities. It seems that there has been a deliberate decision to use a path of historically low resistance for these increased powers of surveillance.

Is there a dividing line between activities that fall under the conditions of this proposed legislation and those that do not? The distinction between entering these words into an application running on my device and using a cloud-based notepad application may be somewhat academic, as they look and act precisely the same way, but under these proposed measures there may a critical difference. Because I use a carriage service to access the cloud-based app then it's quite clearly subject to the provision of this legislation. And to quote from the text "For the purposes of subsection (1), service includes a website." My website is also subject to these provisions. My so-called smartphone is also pulled into this, and I guess my laptop device is also within the remit of this bill because I use it to access carriage services. Ok, so this not actually about telecommunications services per se. It seems to me that this is a very far-reaching bill that attempts to sweep in pretty much all forms of digital activity.

But aside from the rather dramatic reach of this proposed legislation, what's the issue?

The bill provides for "Enhancing the obligations of domestic providers to give reasonable assistance to Australia's key law enforcement and security agencies and, for the first time, extending assistance obligations to offshore providers supplying communications services and devices in Australia." to quote from the bill's explanatory notes. Of course, what is 'reasonable' is a very subjective term, and those folk who have a dim view of the ability of the public sector to exercise restraint when they are not compelled by law to do so will doubtless find a wealth of material in this proposed bill to be concerned about. On the other hand, the picture being painted by the law enforcement agencies of their frustration with various forms of criminal behaviours hiding behind a veil of impenetrable encryption is also a matter of concern. The existing legislative framework is showing its age, and legislation that provides more direct encouragement for digital service providers of all

shapes, sizes and locales to lift their encryption veil when and where possible seems like a timely legislative action.

I attended a session at the Australian Parliament House of the general topic of encryption and security jointly organised by the Internet Society and Internet Australia (https://www.internet.org.au/news/206-event-encryption-experts-evening-canberra-monday-20th-august), and I'd like to share my impressions of the conversation that took place in this session.

MIT's Dr. Hal Abelson noted that accountability is the bedrock of security, and secrecy is the enemy of accountability. He warned that there is a careful balance to be struck here, and we should be careful of mandating vulnerabilities or forcing users to use insecure mechanisms in order to further investigative capabilities. Complexity is the enemy of security, as complex systems tend to fail in complex ways. He pointed out that the issue of encryption has been a long-standing topic of government interest, and it was going to continue to be an active topic of public sector interest.

Encryption is intended to allow to parties to communicate in ways that prevent eavesdropping, tampering or other forms of intervention. It is often seen as a tool for real time communication, such as exchanging messages, but it can just as easily refer to communications over time, such as using an encrypted data store. Encryption has long been a matter of contention between states and their subjects. The state has always wanted the power to covertly eavesdrop upon these ostensibly private transactions. Investigation of criminal activity, or aspects of potential threats to national interests are often powerful motives for state agencies, and often the topic of access to encryption is part of that tension. It appears that a state of nirvana for such state actors would include a level of encryption that would offer some appropriate level of protection of individuals from each other, and from foreign state actors, but permit unfettered access by this state's agents. It's unclear that this has ever been achieved, but there are persistent outbreaks of rumours that various encryption algorithms contain vulnerabilities known only to certain state agencies.

Up until 1996 the United States had declared that any digital encryption using keys longer than 40 bits was classified as a "munition" and subject to export control. Encryption technologies were transferred to the commerce control list and over the ensuing years permitted key lengths were lengthened and more cipher suites were added. It might come as a surprise to some, but US government oversight of cryptographic technology still exists today, and export notification is evidently still required.

The encryption debate continues. One view is that the state should not arbitrarily compel individuals to hand over their passwords and encryption keys to state actors no more than individuals should be compelled to lodge duplicates of keys to their house or their bank accounts. Individuals should have a basic right to privacy, free from obsessive surveillance and arbitrary intrusion into their private affairs. The other side is the view that law enforcement agencies and national security agencies are being frustrated in their efforts to undertake their mission. As the threat levels of hostile digital activities increases, the agencies' ability to investigate, prosecute and defend is being compromised by the ready access to deep encryption that can effectively cloak such hostile activities. This tension is often portrayed as a two-sided issue, between the state and its citizens.

However, it seems that this two-sided tension is no longer the entire story, and the sector of digital service providers has added a third party into the mix. These digital acquisitors have an unquenchable thirst for data about each and every one of us. In only a little more than a decade, they have created a private surveillance apparatus of quite extraordinary reach and sophistication. If personal data is viewed in the same manner as a vein of valuable minerals these data miners, namely Google, Facebook, Apple, Amazon and their fellow travellers, have tapped into the motherlode. This business model, that has been labelled as "surveillance capitalism," fuels the most valuable public companies in this world today. The asset base of these enterprises is our individual profiles, and the value of these profiles is not only what we purchase today, but also what we will purchase tomorrow and what can influence or even drive these future purchases. If this is the asset base, then little wonder that none of these enterprises are acting as if they are willing to pass this data over to state actors for free. These enterprises have so far evaded even the lightest touch of regulatory impost, and if one observes that Google parent, Alphabet, spends more money on lobbying US politicians than any other American corporate entity today, then their objective is quite obviously to ensure that it stays that way.

If this is a three-way tension, then it's clear that we are not equals at the table here. It seems that as users we continually get short-changed when it comes to access to tools and technologies that can allow us to preserve our personal safety and security. In a public key encryption framework, the private key is the critical element. The idea is that this key is never exposed under any circumstances, and instead the framework uses 'proof of possession' techniques that can demonstrate knowledge and use of the private key. This is what is used in secure sessions in the Internet. But this security is provided for the server, not the client. It's server-side encryption that secures the channel. Users don't get the same deal. We are left with a bunch of passwords, and we are forced to constantly use them. Nothing has changed in this picture for more than a decade. Little wonder that large scale breaches of these password tokens occur with sickening regularity.

But I don't think that users are the intended objective of this legislation.

It seems to me that this a conversation about the Australian security and law enforcement agencies attempting to coerce a number of multi-national data acquisitors to expose their core assets to these state agencies on demand.

A problem with this form of coerced exposure is that the users really have no idea what data is held about them in these assembled profiles. The protections users currently have over their profile data is scant enough already. We have no idea who purchases these profiles and how they are subsequently used and capitalised. We have no idea what the consequences may be if this data is also opened up to the state. It has often been observed that the difference between detailed investigation and pervasive surveillance is only known in retrospect. It's only clear that a line has been crossed when we have already crossed it. The concern that these proposals create is that in their efforts to unlock these data lodes for arbitrary state inspection we are unlocking far more than what is healthy for a robust and secure democracy.

A question left in my mind at the end of the session was whether users should be asking way more of encryption and secured data services. Why shouldn't my data be encrypted within the vaults of these data miners, and the only key to unlock the data should be held by me. Why shouldn't I be asked for permission when someone wants to sell my credit card spending records, my online purchasing profile, my browsing history, my logs of DNS queries, my locations, my activity profile and every other aspect of my life that is hoovered up by these digital service providers. Why am I the victim of surveillance capitalism, and why isn't the state using its records to help me rebalance this relationship and empower me to protect my own data? Why is the state spending its time and resources beating its head against the hermetically sealed doors of the data vaults demanding back door access to the keys instead of helping me to regain control of my own data profile?

It seems to me that the European GDPR measures actually went to the heart of today's issues for users. If governments are truly concerned about the security and safety of their citizens, then they are right to be concerned about the cavalier attitude many data acquirers have towards the personal data they hold about users. The GDPR measures appear to create strong incentives to treat this data with all due care and attention. And surely that's something we all would like to see.

It also seems to me that the Australian legislative proposal is heading in entirely the opposite direction. Rather than providing incentives for digital service providers to treat this personal data with due care and attention, these measures appear to want to beat the door down to get a look too!

Here's the material about the proposed bill:

https://www.homeaffairs.gov.au/about/consultations/assistance-and-access-bill-2018
https://www.homeaffairs.gov.au/consultations/Documents/the-assistance-access-bill-2018.pdf
https://www.homeaffairs.gov.au/consultations/Documents/explanatory-document.pdf

Disclaimer

The above views do not necessarily represent the views or positions of the Asia Pacific Network Information Centre.

Author

Geoff Huston B.Sc., M.Sc., is the Chief Scientist at APNIC, the Regional Internet Registry serving the Asia Pacific region.

www.potaroo.net