From: Russell Stuart
To: Assistance Bill Consultation
Subject: Comments on the Assistance and Access Bill 2018
Date: Monday, 10 September 2018 11:53:50 PM

I am writing to comment on the Access and Assistance Bill of 2018.

I am mostly interested in effects of the technology the bill will play out in the long term. To do that it is necessary to speculate on how the bill will be used on a day to day basis.

I am assuming it will be roughly like this:

1. The Law Enforcement Agencies will (LEA's) procure what I will call "taps". I borrowed the word tap it's traditional meaning in: "to put a tap on a telephone". In that case it a tap would be physical device, but in this case it is most likely a software program that captures the required data and sends it back, mostly likely via the internet. The tap will be able to bypass the protections the maker of the device has in place for normal applications to enable it to have full access to all data and sensors on the device.

2. The Law Enforcement Agencies will work with the software makers of the devices they wish to intercept to create a way to install the tap on the device remotely, silently, and undetectably. I assume the software makers will automate this process as much as possible. This isn't a big assumption as these companies (and indeed my job) exists commercially because the can replace human time with computer time. They are very good at it. In fact they are so good at it, I expect over time there will be no human involvement from the at all during the day to day operation of the act.

3. When a LEA wishes to tap a device, if will follow faithfully whatever provisions and protections are in the bill to prevent miss use. I do not feel qualified to comment on whether the current provisions and protections in the current bill are sufficient, but I have enough faith in the strength of Australia Democratic institutions to believe that if the aren't it will be fixed over the long term. To put it another way, when the act is used as it's authors intend, it will work as they intend or will be amended to do so.

Now I would like to introduce you to my world. I am a computer engineer. I build and administer computer systems. I write software, assemble hardware, and do the day to day things required to keep these systems running. The thing I want to discuss here is how the law effects my world.

In my professional capacity, I am mindful of the law and do my best to follow both it's letter and intent. In Australia this means being careful with private data doing my best to secure it, advising my employers on what records they must keep, staying on the right side of Australia's SPAM regulations and so on. All companies I have worked with share my attitudes. And to tilt a hat to the police, government agencies, judges and others who administer Australia's law they seem to be very effective at it. I can't think of a single instance where an Australian entity has got away with openly breaching our laws, and as a

consequence if the world only consisted of Australia my life would be a lot easier.

In contrast to that, it appears other 99% of the worlds population are completely unaffected by our, or indeed anyone's law. Here are some examples from my daily routine:

1. About 1/2 the email my server receives is illegal SPAM as defined by Australian law, which is about average [0]. End users see far less than that of course as the email providers do a lot of automatic filtering to get rid of it. In his heyday Bill Gates received several million SPAM emails per year. [1] I hope his filters are better than mine.

2. Every few seconds someone tries to hack into the web site of the company I work for. We know this because we see the hack attempts in the log files. During the night when normal uses are asleep, almost of all of the requests to the web server are hacking attempts.

3. I run an internet phone server. If someone can guess a user name and password to that phone server, they can place phone calls to "premium" international numbers (which like Australian 1900 numbers earn the caller money). As a consequence our servers get bombarded with attempts to log in using random user names and passwords. It gets irritating because when you are working on the software, the shear number of these attempted calls (often many a second) makes it difficult to see the legitimate calls you are trying to follow.

All these attempts (there can be hundreds per second) are illegal, but I don't bother to report them to a LEA. No one does. No even Law Enforcement Officers reading this document will likely bother to report the SPAM that ends in their inbox, or phone callers insisting they are Microsoft and are here to help, ladies with pretty pictures soliciting for husbands. There is simply no point, because for a variety of reasons there is nothing the LEA's can do about it for a variety of reasons. To mention just a few:

- It's unlikely they will even discover who is doing the hacking because the computer / thing doing the hacking has likely been hacked itself. It is in effect just another victim.

- They have enough problems policing Australia's population. The scale of this is far bigger: it is every cyber criminal on the planet, attacking everyone at once.

- Assuming they did some identify who was responsible, it's likely they are out of reach of Australian law. For example 4 years after Sony's computer systems were hacked to the point all their new upcoming movies where released on the web, they did not know who their employees where, who they owed money to or who owed money to them, they FBI have laid chargers against North Koreans. [2] This will likely have about as much effect as Iran's discovery that it was the USA who destroyed their uranium processing centrifuges by hacking the control software. [3]

Thus my world has two sides. One has its rules determined by the law. The other operates completely outside of the law. But even so this second side is still predictable it in own way, meaning it possible to determine with reasonable probability what is and isn't

likely to happen. If that wasn't so, there would be no internet e-commerce such as internet banking as they could not exist in complete chaos. People build processional livelihoods in learning the rules that do apply in this world, and building systems accordingly. The first thing you have to unlearn is relevance of the law to everyday life. This world is nothing like everyday life.

The rules of this world are hard to intuit. There is for example very little in the regular world that is as certain as 2 + 2 = 4. Yes, the sun will probably rise tomorrow - if a war hasn't triggered a nuclear winter. Yet encryption is just as certain as 2 + 2 = 4. That is because encryption is the same animal: it is also maths, albeit a little more complex than 2 + 2. If a cryptographer says a cipher is unbreakable, then either they are wrong (which because it been studied for decades now is unlikely), or baring a change in the way we understand the universe works will be unbreakable in the time available before the Sun exhausts its fuel.

Yet, the data the encryption guards is probably available despite that. The reason is simple: data that can't be decrypted if you know the right things is useless. There is no point having an encrypted message no one can read, or a digital signature no one can sign something with. To provide one example of this: there was once a smart card called Mondex. [5] Mondex was a smartcard, but unlike todays smartcards it didn't rely on a balance stored by a bank. The balance was stored in the card. This meant it had to be near perfectly secure, as if someone could alter that balance they could effectively print money. MasterCard went to a lot of trouble to prove it was cryptographically secure. Unfortunately the card had to be able to alter that value, which means the secrets that cryptography depends on had to be stored on there too. However is nothing particularly new about this: your paywave card knows your PIN. In fact the EFTPOS terminals need secrets too, and they are also protected by chips very similar to the one in today's smart cards. Ditto the SIM you put in your telephone. This is safe because these SIM's we rely on are obviously very, very hard to hack. In fact clearly the makers of Mondex considered them to be perfectly secure. But to be sure, they put a few million in prize money out there for the first person who did hack it. Some microelectronic university students in Ireland did it - they burnt new tracks into the chip using an electron microscope.

The Mondex example hides as much as it reveals. In Mondex's case the equipment needed was probably worth more than the prize, the millions in prize money was probably far less than the engineers would earn over their lifetimes. In reality, that is very rare. But it does show that like humans, every piece of equipment does have its price. Given some time, and enough money, that means the secrets needed to secure encryption are stored somewhere they can be extracted. There is even some flexibility on how you spend that budget. You could spend it on breaking hardware (although in reality what happens is lots of people have a go, and eventually one succeeds). Or you could spend it on bribery and espionage, which is usually the easier path.

If everything is breakable, how do you secure something? There are lots of tricks, but it boils down to one rule: what you are protecting has to be worth much less than the rewards of cracking it. The rule is so good it can be used to predict behaviour. For example, criminals involved in ramsonware have been known to do price testing, which is to say they have been seen to vary the price charged to similar organisations in order to learn the price that will maximise their returns. Banks take advantage of this rule by reversing fraudulent

transactions. Since everything up until the money is converted to cash is reversible this limits their liability to what can be carried away in cash. Provided you notice the fraudulent transactions quickly, it puts a pretty low limit the losses. If you don't notice quickly, well then the losses can be huge [5].

The solution to humans having a price is a little different. The price is not only money. The USA Democrats emails were leaked because of a very well crafted email sent to just the right person. [6] It lead to them entering the password into a rogue server. Google & Facebook have lost a hundred million to the same thing. [7] The price in that case is not money: it is careful research into email addresses, the names of wives, bosses and other social minutea, and of course the patience to do it over and over again until it succeeded. For $100M you can afford to be patient, I guess. The solution is to make success depend on turning a lot of humans. For example, when the TIA act (1979) was enacted, obtaining a tap was a manual process. It would have involved the Postal and Telecommunications Department creating a work order, the work order winding its way down to a technician who installed the tap. If you managed to turn all these people, you got yourself one tapped telephone which you somehow had to make money out of. No one to my knowledge bothered trying.

Which finally brings me to this proposal. The world is now very different to the one the Postal and Telecommunications Department was operating in. The explanatory notes for the act go to some length to say the LEA can not introduce a systemic weakness. This is a good thing. Removing the jargon, it means the LEA's can't demand everyones phone have a backdoor installed so the phones are as secure as they are now. Which is to say: not very secure. Here is an example of why: a year or two ago I was woken up every night at about 2PM for a week by my wife's phone playing some raucous tune and displaying a casino ad (which is of course illegal). This was very odd as my wife swore she had not installed any new software on it, and that seemed to be the case. After some Googling I discovered miscreants had been offering to purchase the packages of Android Play Store apps that weren't making money any more. They then altered the game (in my wifes case) to display this ad during the day USA time. This was in game(s) we had trusted for years. Yet it became a virus. And that virus was installed without us knowing. I still don't know which game it was as I uninstalled them all and that fixed the problem.

The reason the act doesn't need a systemic weakness is it already has one available: the auto upgrading of software. If you can silently install a tap that can access the data when it is not encrypted, then why bother breaking the encryption? Just create a law that can compel the software developers help create such software and you will have access to much more than the data. You can turn on microphones, enable cameras, obtain GPS positions. What's more every device that automatically install security patches (which is currently considered industry best practice) can be turned into a tap. This means PC's, TV's, cars, security cameras, even robot vacuums can be used as surveillance devices.

In fact you don't get access to formerly encrypted data. You get access to everything because you can intercept passwords, PIN's, finger print readers, face scanners - this is literally everything. There is nothing that can be secured against this technology - banking passwords, keys that secure web sites, company confidential emails discussing billion dollar takeovers, currency devaluations. It all becomes an open book to someone who can unlock this system.

Sadly using the technique the banks used to fight fraud, early detection, may be difficult. Copied data looks identical to data that isn't copied. When your secrets are stolen, you still have them. Unlike the money stolen from your bank account, you are unaware they have flown the coop. Provided the effects are kept quite, you will never know.

Once the system is in place, the law will have a lot to say what can be done lawfully. But it will have no impact on what will be done with it unlawfully once it is available. As an example it would matter little if law said the LEA's can't develop taps that record banking passwords or required 10 judges and ministerial approval to do it, because it won't be the LEA's taps. Once this system is in place, it is the rules of my second world that apply.

To recap, those rules ask what is the reward for breaking it, and how hard is it. The reward is likely to be trillions. As for how hard it is to break: these systems will consist of software, just like the software in the phones and other devices the LEA's hope to intercept. Just like the phones, this software will have bugs and need enhancements. If it is business as usual, the software will be proprietary - the Australian government will not be allowed to look at it. The software will be under the control of a bunch of programmers, all operating under time and monetary pressure. There will be a bunch of different things that need to be controlled - source code, to a lot of devices, signing keys, passwords. Not even Google could keep it's $100M safe under those conditions.

If the government wishes to proceed with proposal regardless of this risk, I have one suggestion: insist the source code to the system, or critical bits of it anyway, be open source. The strength of open source is not the price. It's that many people look at it. If just one notices a nefarious change, it's game over. Thus open source embodies the one solution we have to every human having their price: involve lots of independent people.

[0] https://www.statista.com/statistics/420391/spam-email-traffic-share/

[1] https://en.wikipedia.org/wiki/Email_spam#Highest_amount_of_spam_received

[2] http://time.com/5388639/north-korean-charged-sony-hack/

[3] https://en.wikipedia.org/wiki/Stuxnet#United_States

[4] https://en.wikipedia.org/wiki/Mondex

[5] https://www.securityweek.com/hackers-hit-100-banks-unprecedented-1-billion-cyber-attack-kaspersky-lab

[6] https://www.businessinsider.com/new-evidence-shows-hillary-clinton-campaign-chairs-email-was-hacked-in-a-phishing-scheme-2016-10

[7] http://fortune.com/2017/04/27/facebook-google-rimasauskas/

--
Russell Stuart
Address: [redacted]