Submission to the Department of Home Affairs on the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018

To the Honourable Members of Parliament,

For over 30 years I have worked in information technology, and, in specific, within the field of information security (or "Cyber Security" as it is currently known). During that time I've had the privilege to work with tens of thousands of everyday people who are using technology to improve their lives.

And it is with that experience in mind that I write to you regarding my grave concerns over your proposed legislation "Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018" that is currently being considered.

You will no doubt hear from many other concerned parties with respect to this legislation; the entire technology industry is united in unease regarding the breadth and depth of the details. I sincerely hope that you take heed to the global concern that has been generated by this proposed legislation.

However, I wanted to focus on the impact that these proposals have for our citizens, your constituents, and ensure that you hear the voice of the real Australians who will be significantly put at risk should this legislation proceed.

During the course of my work I interact with a vast array of technology users across Australia. From students and retirees to heads of multinational corporations. These are all people who are concerned about their online safety, who read about privacy breaches with great trepidation, and who have been personally impacted by inadequate security protections online.

Many have been impacted by malicious software which compromised their personal computers or smartphones - instantly exposing their most sensitive and private information to criminals. To learn that everything that you say, every picture you've taken, and every piece of information that passes through your most intimate of devices has been accessed by unknown individuals is a powerfully personal invasion.

These devices and technologies have become inextricably linked with our daily lives, so much so that many people may form an almost emotional attachment to their personal computers and other devices.

I recall one recent event where I had to inform a customer that their mobile device was thoroughly compromised by criminals. The only way to "repair" it was to replace it. All trust in the device itself was permanently destroyed. However, this individual couldn't bring themselves to dispose of the device, as it was a gift from their child, and it had a powerful sentimental meaning. The device sits unused, off, in a drawer, as the trust was eradicated, but the emotional connection remains.

The proposed legislation puts all Australians at significantly greater risk for their personal safety, their financial security, and significantly erodes trust in our digital future.

And that is the key word here: Trust.

I was recently reminded of a quote from Sophocles: "Trust dies but mistrust blossoms."

The proposals you are making, and the justifications for them, has become a well-fertilised blossom of mistrust.

Mistrust that you, as representatives of the people of Australia, have in Australians.

Mistrust that you, as our elected government, have in a strong digital economy and society.

And acutely, this blossoming mistrust you are fuelling has impacted our faith and assurance in you as well.

Worse still, the actions you are attempting to force upon technology companies, and the powers you are giving an already extremely powerful law enforcement community, are creating deep

misgivings in the phenomenally enriching technology which has enhanced lives across Australia and around the world.

The vast majority of people in Australia are good people, people who want to know that their personal information is secured and encrypted and kept from prying eyes (including yours). Their "secrets" are mundane compared to the threats you purport to be concerned with, to be sure, but the impact of the broad and invasive legislation, as proposed, significantly endangers all Australians, for the sake of an extreme minority of corner or edge cases.

There is no questioning that some of those scenarios may present a significant threat to Australia, but, the planned legislation puts in place a far greater risk to our privacy and security at a vastly disproportionate level.

This peril is not esoteric. It is concrete, and it has already (repeatedly) come to pass.

Take the case of the United States government and their similar approach with the "EternalBlue" NSA generated computer exploit. When exposed by the "Shadowbrokers" it resulted in one of the most costly IT security events to date: over $8 billion dollars (USD) worth of global damage due to WannaCry alone (which was based on this exploit). A single variation of this "intelligence community" created exploit (known as Not-Petya) cost a further estimated $850 million USD worth of damage.

Your legislation is creating just as significant of a global menace. By empowering law enforcement to behave indistinguishably from the criminals they are meant to pursue, it is all but certain that their efforts will lead to a truly catastrophic outcome. The interconnectedness of technology systems and platforms ensures that unintended consequences, such as WannaCry, will befall us all.

Instead of developing frameworks for eroding privacy and decimating security, government should be striving to protect its people from threats, online and off. Invest instead in more robust encryption and privacy algorithms which prevent criminals from accessing our sensitive information, from accessing our money, and from disrupting our lives. Encourage technology companies to handle information with the most stringent of security guidelines. Demand that information be as tamper proof as is currently possible.

Reinforce, don't reduce.

As I mentioned previously, during my decades working as an IT security specialist, I have come to know countless people who have had their lives impacted by technology - most for better and some for worse. The heartbreaking stories of pensioners having their superannuation funds obliterated through online insecurity and the myriad of daily reports of individuals and businesses having their identities compromised online are tragic and painful. The sense of violation and loss that is felt when private information is exposed and accessed without consent is intense.

Yet these are also examples where improved security, increased use of strong cryptography, and individual-managed privacy controls could have been used to protect and preserve. A stronger and more robust security infrastructure would help in keeping the pernicious threat of online crime at bay. If our information is impervious to unwanted access and manipulation, we all win.

There are also those who have used modern technology to enrich their lives in unexpected and wonderful ways. Making a connection to another person, finding love, keeping in touch with distant family and friends, finding secure and confidential support at times it's most needed — these are the people you are directly putting in harm's way with the proposals.

I have worked with hundreds of people who have domestic protection orders and whose lives are in direct risk should their personal information be accessed online without their full awareness, control, and consent. Similarly, people struggling with the crippling effects of substance abuse or depression, or those exploring their own gender awareness and sexuality, or any number of other equally sensitive and personal issues, need to know that their privacy is respected above all else as they seek support, guidance, community, and advice. They need to know that their online communications are sacrosanct. The violations that this proposed legislation make possible could be life-altering, or, worse, life-threatening.

Hardly a week goes by that I don't hear from someone in their 70's, 80's or even 90's who have concerns and doubts about online technology. "Is it safe?" they ask, "is it secure?" These are people who use iPads and FaceTime to talk to loved ones on the other side of the planet, and they are rightly concerned that their private conversations stay private.

The bill that is being proposed will force professionals such as myself to answer "no, it is not safe. It can not be trusted. It has been weakened by the government, the people who you elected to protect you."

These same concerns are echoed across all age groups and demographics. There is an innate desire to feel in control of your information, of your privacy, and of your personal security that we all crave.

Today, when asked about online security, I can still answer in positive and uplifting terms. Most technology is safe, it is secure, it hasn't been knowingly compromised in any way, and it's only getting better with each new iteration.

Companies such as Apple have seen this and know how important security and privacy is to their customers. As the world's first trillion dollar company, the success of their approach, and the moral and ethical imperative that drives many of their security and privacy decisions, speaks for itself. Millions upon millions of Australians have chosen to be included in Apple's environment, and many have done so explicitly because they know of the focus on keeping information safe and secure.

In my own work, I frequently hear from residents of retirement homes, from owners of businesses, and from those involved with social clubs and other organisations who take my feedback and proudly display it on noticeboards or circulate it for their membership and community to see. People want to be informed, to feel protected, and to feel that their sensitive information is secured.

This is what technology is meant to do; it's meant to bring us together, to unite us. It's meant to give us same level of comfort and confidence when talking online as we have in our homes, in our workplaces, and for some, in their places of worship.

Technology lets us extend these trusted interactions beyond our immediate walls to those we connect with around the globe. Technology has become perhaps the most powerful tool humanity has developed, and the good that it has done is without equal.

Yet it is just a tool, and without doubt, there are those who would use the same tool for malevolent purposes — after all, a wrench is just a wrench, it's the criminal who makes it a weapon.

The Australian government has already enacted some of the most invasive legislation on the books; between mandatory data retention to lawful interception to the inability for someone to simply buy a telephone without having to hand over copious amounts of highly personal identity data — there is absolutely no shortage of data, of tools, or of resources for the law enforcement community to make use of in order to protect all Australians.

More is not needed.

Those who whisper in your ears over the threat of "going dark" and the risks associated with their increasing inability to invade, intercept or manipulate our private lives are paid to plan for the worst case and to hyperbolise drastic outcomes. They are the corner case built on mistrust. Heeding their pleas for more access and the ability to violate the security and privacy of every individual in Australia (and, by extension, the world) is an unreasonable acquiescence.

However, I am not naïve, I know that there may well be instances where law enforcement truly believes they would benefit from this increased access through the circumvention or violation of security measures in order to prevent a genuine disaster - yet even with those best of intentions, the global consequence needs to be taken into primary consideration.

The whipped cream is out of the can with respect to cryptography. The massive number of data breaches occurring around the world has created a fundamental shift in how organisations are expected to collect and secure information. "End to end" security, without diversions, without

backdoors, without enforced government assistance, without compromise, is what the people, the people who you are here to protect, truly need, and are increasingly demanding.

Every day better and faster ways are developed to keep information secure and private, and that trend is necessary to further the economic and personal prosperity which our digital era enables.

Rather than looking for ways to break security in the name of security, an irony which I truly hope you are not blind to, invest instead in technology development which can keep Australian's data secure and impervious to attacks against it.

Focus on keeping not just your secrets secret, but ours as well.

In lieu of asking providers of technology and communications services to weaken or modify their services at your behest, consider, alternatively, asking them to make them tamper-proof and resistant to any form of unauthorised access or modification. Work *with* service providers to help ensure that the integrity and sanctity of our information is firmly intact and kept out of the hands of criminals and those who would do Australians harm.

There is a remarkable opportunity to do good here. Just as the vast majority of Australians are good, this is your chance to show you are one of us, not one of "them." Show us that you trust us, and that you deserve our trust. Unite us, do not divide us further.

One should never behave like criminals in their attempt to address criminality — but this is precisely what the proposed legislation does. You can do better, and we certainly deserve better.

As a society, we are living at the precipice of amazing developments in the world of technology and online communication.

Where once it took weeks or months to communicate with the other side of the world, now we can write, talk, even have face to face video conversations with just about anyone, anywhere. The promises of embedded communication in even more devices (often referred to as the Internet of Things) pushes these possibilities even further. Advances in telemedicine provide medical expertise to even the most remote amongst us. In education, high speed Internet has fostered global communities built on open discussion, unifying minds and experiences across Australia, and beyond.

But these promises of the future are contingent upon the ability to deliver a secure solution which is trusted by the public. The legislation that you have proposed shows not respect for said public, but contempt.

However, it's not too late. In a time where political divisions have never been greater, and we, as citizens, have never felt further from those in a position of power, you can show us that you hear us, that you do respect us, and that you will protect our rights, our security, and our privacy, in a truly meaningful way. This legislation needs to be significantly modified to enhance our digital security and privacy, or it needs to be dropped entirely.

Instead of listening to the pessimistic whisperers who plant the seeds of mistrust, fear, uncertainty and doubt, listen to us, the vocal majority, the good people of Australia, who clamour for online security and confidentiality.

Now is the time to act in a positive, privacy and security affirming manner. Embrace education and awareness, solidify secure communications and help make Australia a respected leader in the digital era.

Thank you for your time and consideration,

Scott A. McIntyre
[redacted]