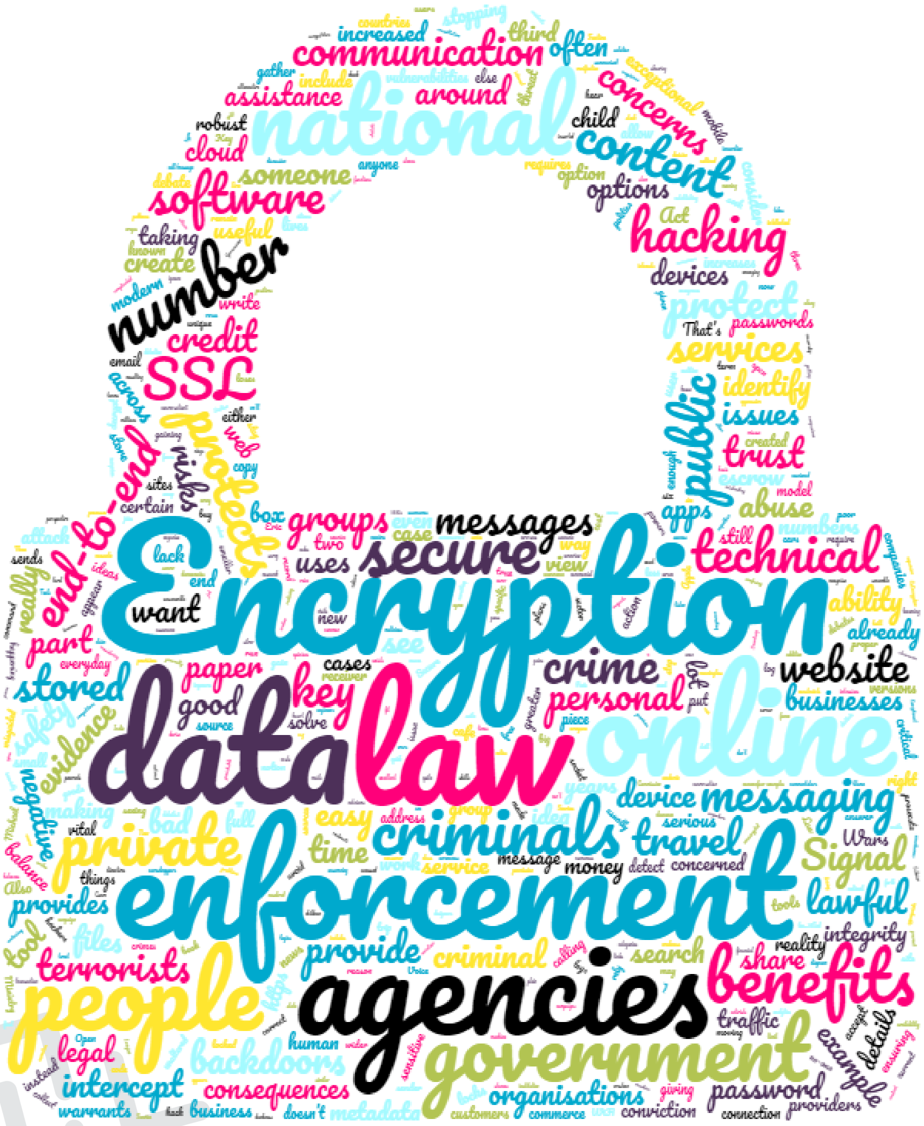
Encryption: ways forward that protect the Internet's potential

An InternetNZ position paper



InternetNZ

InternetNZ

Executive summary

Encryption is everywhere in the modern Internet. We rely on it to facailitate communications, store information privately, control access, authenticate, protect online banking information, credit card information and more.

However, while encryption has brought us all huge benefits, criminals and terrorists are also using encryption technologies to communicate, plan and organise crimes and acts of terrorism.

And there lies the problem, encryption improves our information security, but criminal use of encryption technologies create some national security and public safety risks. Encryption is not alone in this: cars, guns and baseball bats have also been used by criminals and terrorists.

There are now many conversations taking place globally about taking steps to address the negative consequences of encryption. Some ideas have been to create law that allows back-doors to be created so that law enforcement agencies are able to intercept encrypted information in the case of a criminal conviction. Some have even talked about banning encryption technology all together.

However, ideas like these would have terrible consequences for the security and trust of the Internet.

The question that needs to be answered by our society is whether the Internet or information security benefits created by encryption are seen as more valuable than the smaller number of national security risks that are complicated by encryption. As a country, we also need to consider whether these risks can be addressed through other means in order to realise the security benefits and wider economic and social benefits of encryption.

The reason for writing this paper is that we think conversations need to happen in New Zealand to start gathering information and answering questions like these ones.

We don’t accept that solving challenges relating to encryption is a zero-sum endeavour, with one side gaining what the other side loses. We think there are options for increasing New Zealanders’ security online and also addressing the concerns of law enforcement and national security agencies.

These are options we would like to explore for the better of the Internet and all New Zealanders.

We are committed to working with the technology sector, the New Zealand Government, civil society and academia to get the right conversations about encryption happening.

We have written a corresponding paper to this one titled ‘Encryption: what it is and why it’s important.’ It explains what encryption technologies are, why they are useful and why they are an important part of protecting you, and your information online. It also outlines that encryption technologies are being used by bad actors and explains what some countries are doing to try to stop this. You can read the discussion starter at: https://www.internetnz.nz/encryption

We are being asked to balance privacy vs security...but that notion of balance is misleading

We often hear about encryption being a privacy vs security debate. But we think that is a false dichotomy. Encryption is a security technology that protects privacy. Encryption technologies support technical security, communications security, human security and business security.

However, the use of encryption by 'bad actors' does have an impact on national security. Therefore, as the USA's staff report to the Senate Committee on Homeland Security put it:

> ***"the issue is really about security versus security: encryption protects critical infrastructure, trade secrets, financial transactions, and personal communications and information. Yet encryption also limits law enforcement's ability to track criminals, collect evidence, prevent attacks, and ensure public safety."***[1]

The claim that encryption is a security threat, or a security cost, is only true if you are only thinking about national security – and then only some of the time as defence and intelligence agencies rely on it to keep information secure. From any other security perspective, encryption is a benefit, not a cost.

The true security vs security trade-off for encryption is whether the Internet or information security benefits created by encryption are seen as more valuable than the smaller number of national security risks that are complicated by encryption. We also need to consider whether these risks can be addressed through other means in order to realise the security benefits and wider economic and social benefits of encryption.

What options have been suggested to date?

Internationally, people have been debating what to do about encryption. Driven by concerns from law enforcement and fears about national security, politicians and commentators have been trying to solve the national security risks. The common solutions that we have seen suggested and debated in the United States, and other countries are:

- government backdoors into encryption software and platforms
- key escrow (giving a copy of your keys to a trusted third party)
- banning encryption technologies.

Each of these ideas has its own problems, most of which stem from a false assumption about privacy vs security, and are summarised on the following page.

[1] Staff report for Senate Committee on Homeland Security. 2016

Government backdoors into encryption software and platforms

One recurring suggestion has been to require organisations deploying encryption to put in place government backdoors, or exceptional access that allow government agencies to access encrypted content without user permission.

Exceptional access provisions are misguided and damaging to information security. They effectively ask technologists and service providers to assist (national) security services by reducing technical security for all. If an encryption tool has a backdoor or a weakness in it, there is no guarantee that only the government and the designers will know about it. Hackers, foreign governments and organised criminal groups will do everything to identify and exploit the backdoor for their own purposes. If a backdoor exists then it can be found and once found it can be used by anybody who has it without anyone else knowing.

Also problematic is which governments should have access? In the United States, the argument is based around a robust, criminal justice system with a number of checks and balances against executive government overreach. In New Zealand, such a proposal would also be subject to our legal systems. However, if the United States, and other liberal western democracies like New Zealand start requiring backdoors then how could the same organisations credibly say no to authoritarian or oppressive governments?

We think the idea of mandating backdoors, or exceptional access for government agencies or law enforcement, is a bad one. It degrades the overall security and utility of encryption technologies. It only appears attractive as it's seen as an easy (for the government) option when taking a very narrow view of national security interests.

Key escrow

Key escrow is an idea whereby software companies ensure the information their software encrypts can be decrypted with a specific decryption key. This key is held by a third party (not the company and not the government) that law enforcement agencies can seek decryption authorisation from following a search warrant or production order. Often, the judiciary or a technology institution is raised as a possible third party to administer key escrow.

The main issue here is that again, you are asking cryptography service providers to create additional opportunities for the decryption of the information the software or hardware protects. Further to this, that third party will become a hugely attractive target for hackers and intelligence agencies. Given the poor record that many government agencies have on information security practice, and the sophisticated threat model that such a service would have, it would likely be breached and the escrowed keys to a number of services would likely be copied by intelligence agencies or criminal groups for all sorts of nefarious purposes. These could then be used without anyone knowing.

Examples of government sector data breaches

- The US Office of Personnel Management was hacked up to six times between 2013 and 2015, resulting in the loss of the security clearance forms of a huge number of United States Government officials (past and present) with security clearances.
- In November 2014 the US Postal Service had a data breach for 800,000 employees personal information, as well as email.
- WINZ's kiosk breach: a journalist was able to access sensitive information in the New Zealands Ministry of Social Development (MSD) corporate network due to poor security.

Banning encryption technologies

Not only is the idea of banning encryption for business or personal use damaging to security, it is short-sighted and pointless. Banning technology doesn't work as people invariably find ways to access it. In the case of cryptography, the maths behind it is very well known and someone sitting in their bedroom can write high quality encryption software without any help. We live in a networked world, with easy to access virtual private networks. Tools like Streisand[1] and Algo[2] can be downloaded from Github for free and enable you to run a suite of privacy and obfuscation tools that can get around Iranian and Chinese monitoring and censorship.

Encryption is a global technology. There are numerous solutions, including freeware and open source encryption technologies that an individual can get access to.

The reality is that consumer-accessible encryption technologies are here, and they are here to stay. What we need to do, as a society, is identify and discuss possible options to help mitigate the negative consequences of widespread encryption technologies.

We need to remember that New Zealand is a technology taker...

Even if these options were actually viable, can New Zealand actually affect global encryption technologies? A 2016 survey of encryption products found that there were over 850 hardware or software products available from companies in 55 countries.[3] Of these, only four are from New Zealand. Organisations and companies from all over the world offer encryption services, tools and technologies.

This means that policies or suggestions that seek to undermine encryption, or force specific corporations to weaken encryption are not likely to have any impact in New Zealand. We do not have a sufficiently large market, nor do we have the providers here to influence or demand action from. We need to figure out solutions and options that reflect the market and technology realities we face.

[1] Streisand is a free software suite you can find on Github here: https://github.com/jlund/streisand

[2] Algo is a free VPN that you can download and run yourself: https://blog.trailofbits.com/2016/12/12/meet-algo-the-vpn-that-works/

[3] B. Schneier, K. Seidel, and S. Vijayakumar (2016) A Worldwide Survey of Encryption Products https://www.schneier.com/academic/archives/2016/02/a_worldwide_survey_o.html

‘Going dark’ or pockets of darkness?

As stated in our encryption discussion starter, going dark is a term law enforcement and surveillance agencies use to describe situations when they have the legal authority to intercept or access information (such as communications content, files and content on a phone). This authority usually comes from a search warrant, interception warrant or production order, but they lack the technical ability to do so. Encryption technologies are usually the reason for law enforcement going dark in a particular situation.

However, many law enforcement agencies are using the term going dark to describe a broader trend – that they are technically able to access less and less information and that this lack of access and visibility is creating significant public safety and national security risks.

In reality, a lot of information isn’t going away and new techniques are emerging

As set out on page 12 of our encryption discussion starter, this general fear is based on a number of specific cases. However, a lot of information isn’t going dark, because it’s critical for businesses and service providers to maintain their visibility. Site data analytics, machine learning, targeted advertising, and chatbots for customer support all rely on access to content as well as metadata. Many organisations will not put in place end-to-end encryption everywhere – it’s not in their business model to do so.

Currently, roughly 18% of global Internet traffic is end-to-end encrypted. This is expected to grow to 22% by the end of 2019. Currently, storage encryption on mobile phones sits at about 47% in the United States.[1]

Access to communication content is declining, however metadata (see the ‘what is metadata’ box on the next page) will still provide a rich analytical tool for investigators and intelligence agencies. In one study, an academic team could identify an individual 90% of the time in a group of 1.1 million across three months of credit card records with only four transaction records showing time and place.[2] Metadata is very powerful and can be used to identify persons of interest, establish patterns of activity, build up pictures of relationships, and create potential opportunities for monitoring and physical location-based wiretaps.

[1] https://www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data

[2] http://dx.doi.org/10.1126/science.1256297

What is metadata?

Metadata is data about data. In the context of communications data, metadata (sometimes called call associated data) includes information like call/message time, sender and receiver phone numbers, IP addresses, duration of call, and the geo-location of sender and receiver. Metadata is generated by the activity of communication, and is generally not encrypted. Metadata is a hugely useful intelligence tool.

Also, the Internet of Things and an increased number of Internet devices in the house mean that if a target's mobile is too hard to intercept, their TV or fridge microphone might instead be used to record conversations.

We understand that law enforcement agencies want to protect their ability to read and listen to data they collect under a search warrant. We empathise as this new and growing technology is creating challenges for law enforcement agencies. They want to keep operating in the same ways that they have over the past few decades where they can leverage the investigative benefits of the digitisation of a large amount of information, but without the negative consequences of the technologies needed to protect this digitised information.

We think that, whenever you stack up the positives and the negatives of encryption, it's a clear positive. And we're not alone in thinking this. Even someone like General Michael Hayden, who's been both NSA and CIA Director, thinks trying to fight against communication encryption isn't a good idea:

> **"Give up content. Content is going away. There is a natural arc to technological progress that's going to make content more and more and more difficult to extract from communications...accept that reality, decline gracefully and begin to gather information... which is still available"**
>
> **- General Michael Hayden[1]**

Therefore, given there are concerns, and there clearly are some national security and public safety issues, what are some good ways of dealing with that?

[1] https://www.lawfareblog.com/video-gen-michael-hayden-his-hoover-book-soiree

New Zealand should explore lawful hacking for serious crime investigations

If going dark is really going to happen – and law enforcement will not be able to access plaintext versions of content they have warrants for – how will they continue to do their job as investigators?

One answer is to enable ‘lawful hacking.’ As outlined by Susan Hennessey, from the Brookings Institute:

“Instead of creating additional vulnerabilities to an already fragile security ecosystem in the form of exceptional access...law enforcement should exploit existing vulnerabilities in software and hardware.”[1]

Lawful hacking recognises that organised criminals such as child sex abuse rings, terrorists and transnational crime groups, are technologically savvy and security focused. They are not likely to be undone by exceptional access into encryption software – with hundreds of choices they will be guided by what is secure, not what is easy to use. In the Playpen case, the use of hacking tools enabled the FBI to identify over 35 individual offenders who had committed actual child sex abuse, as well as enabled them to identify and rescue almost fifty children from ongoing abuse. That is clearly a societal good.

In New Zealand, enabling lawful hacking would effectively mean giving New Zealand Police the authority and resources (or access to the skills) to ensure that they can hack devices that they have lawful warrants to access the data on, but for which they cannot gain access through any other means.

A lawful hacking policy is complicated and requires clear policy directives, codes of conduct, a process for how agencies deal with security vulnerabilities[2] and proper constraints to avoid issues around mass hacking warrants and as-yet unidentified concerns. Issues with lawful hacking include:

a. it is not likely to scale well (given New Zealand’s size, this may not be as big an issue for us as others)

b. it can be expensive to buy or find exploits (a full iOS exploit can command a price over $1m USD)

c. requiring significant investment in a competitive market (hackers can command high wages in the information security industry) that law enforcement agencies such as New Zealand Police have not operated in in the past.

We should also be discussing what categories of crime it is permissible to use lawful hacking in. Should it be only a small group of the most heinous crimes (for example murder, sexual abuse and terrorism)? Or should it be available for the investigation of serious crime (crimes punishable with imprisonment of five years or more)?

Lawful hacking is not a silver bullet, and there are plenty of potential human rights and misuse issues that need to be worked through. But we think it should be actively considered and explored as a ‘not as bad’ alternative to backdoors.

[1] Susan Hennessey, p12

[2] The USA has a Vulnerabilities Equities Process where the NSA disclosed to vendors some 90+% of the security vulnerabilities they found or were made aware of

Powers to compel assistance to access devices are likely to be part of the solution...

...but not the whole answer. New Zealand already has legal powers to compel assistance on the statute book. Section 130 in the Search and Surveillance Act 2012, the Customs Act has compulsion powers, as does the Anti-Money Laundering and Countering Financing of Terrorism Act 2009. In the case of encryption, one possible option is to require a person to provide assistance to law enforcement to decrypt information. There are some obvious human rights issues associated with self-incrimination, the state forcing citizen action, especially without reasonable grounds.

As well as considering and debating technical access requirements, New Zealanders could look at compelled assistance duties as another way of mitigating the law enforcement negatives of ubiquitous encryption. If New Zealand was to examine this option we think that some questions to consider include:

- Who should be able to compel assistance? Law enforcement officers or should a court order be required?
- In what circumstances would compulsion be considered proportional, appropriate and reasonable?

The Law Commission and the Ministry of Justice are currently reviewing the Search and Surveillance Act, including its compulsion to assist power. Their analysis and research could be an important first step in exploring whether this option could be viable for New Zealand.

We need more information

One of the challenges in any debate around encryption is that there is a lack of information. We know the upsides of encryption, but the negatives are not as easy to understand, and are murkier.

Before anyone starts "doing something about encryption" (whatever that actually means), we think we need a lot more data and information in order to have a proper debate and discussion.

We, as a society, need to have answers to a whole lot of questions before we can start thinking about which solutions and trade-offs to make.

- In how many cases has the New Zealand Police actually been thwarted by encryption?
- What percentage of serious crime investigations was that?
- Were they still able to achieve a conviction?
- Were there other sources of evidence they could use / did use?
- How often are national security investigations stopped or discontinued due to device encryption or end-to-end encryption?

Until we have good information and statistics, we think we need to pause and not rush in.

Our position on encryption

We think that encryption is not only vital for businesses and governments, but it's vitally important for modern life.

We all have information we want to keep private. We think that trust in the Internet is a very important piece of the puzzle to unlocking the benefits and potential of the Internet. Encryption helps bolster trust through providing confidence in correctness (that you really are communicating with the computer you think you are), privacy and security.

We do not accept that solving challenges relating to encryption is a zero-sum endeavour with one side gaining what the other side loses. There are options for increasing New Zealanders' security online AND addressing the concerns of law enforcement and national security agencies.

We want:

- New Zealanders to have great, easy to use, encryption available so you can protect your information and communication. That's why we've produced our private message resources, to encourage New Zealanders to use private messaging apps that use best in class end-to-end encryption technology. [1]
- A world without mass surveillance: encryption is an important part of stopping the Internet being used as a surveillance tool. That's why we're working to support the Electronic Frontier Foundation's game plan for ending global mass surveillance.[2]

To work towards this, we will:

- Run public awareness campaigns (like our private messaging apps campaign) to encourage New Zealanders to use encryption technologies in their everyday lives.
- Speak up for the benefits of encryption and other security technologies whenever someone tries to portray only the costs or negatives.
- Make all our websites default to https: we commit to running secure socket layer (SSL) encryption on all websites we run (including NetHui sites) and we'll redirect people to the https connection wherever possible.
- Share our encryption paper, the analysis and recommendations with key decision makers and reach out to government, business, academia and civil society to have a genuine, informed debate about encryption's benefits, risks and how we can work to mitigate risk without undermining trust online.

[1] https://internetnz.nz/myprivacy

[2] https://internetnz.nz/towards-world-without-mass-surveillance

About InternetNZ

InternetNZ's vision is for a better world through a better Internet. We promote the Internet's benefits. We protect its potential. And we focus on advancing an open and uncaptureable Internet for New Zealand.

We provide a voice for the Internet in New Zealand and work on behalf of all Internet users across the country.

We are the designated manager for the .nz Internet domain. And through this role we represent New Zealand at a global level.

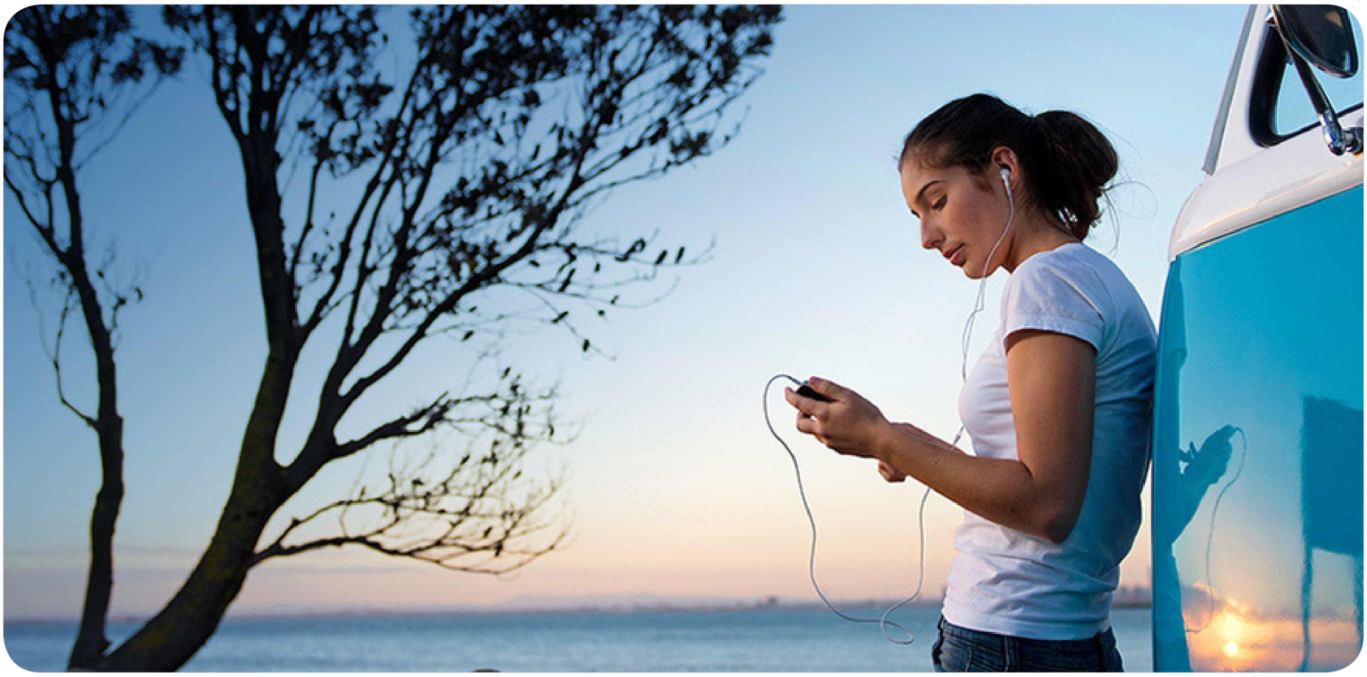
We provide community funding to promote research and the discovery of ways to improve the Internet. We inform people about the Internet and we ensure it is well understood by those making decisions that help shape it.

Every year we bring the Internet community together at events like NetHui - to share wisdom and best practice on the state of the Internet.

We are a non-profit and open membership organisation.

Be a member of InternetNZ and be part of the Internet community.

You can keep a close watch on the latest tech and telecommunications developments and network with other like-minded people at cool events. Being a member of InternetNZ only costs $21 per year. Find out more at internetnz.nz/join



InternetNZ

InternetNZ

Level 11
80 Boulcott Street
Wellington 6011

P.O. Box 11-881
Wellington 6142
New Zealand

Free phone: 0800 101 151
Phone: +64 4 472 1600

www.internetnz.nz

@InternetNZ

InternetNZ