Privacy Commissioner
Te Mana Mātāpono Matatapu

IAPP ANZ Summit 2019 keynote presentation

NZ Privacy Commissioner John Edwards

Addressing the Power Asymmetry of the Big Tech Companies

30 October 2019

Introduction

Last year in Auckland, a young English backpacker, Grace Millane hooked up with a man on Tinder, the day before her 22nd birthday, went on a date, and went missing. Her parents were concerned when she did not respond to birthday messages and notified New Zealand Police three days later.

On the 8th of December, a man was arrested and charged with her murder, and Grace's body was recovered the following day.

The accused appeared in the Auckland District Court on 10 December. An application for name suppression was made and denied by the judge. The defendant's counsel appealed that decision, which meant that automatic name suppression came into effect. Name suppression prohibits publishing the name or identification details of a person before the court.

A breach of name suppression is a contempt of court, but one which cannot be enforced outside the jurisdiction. Several international media outlets ignored the order and published the details of the defendant's identity.

This led to a large number of online searches relating to the case, and specifically, to the individual charged with murder.

Somehow the level of interest attracted the attention of Google's "trending topics" algorithm, and the details of the defendant's identity were pushed out in an alert to New Zealand subscribers in breach of the suppression order.

Suppression orders are made to preserve the rights to a fair trial. A failure to deliver a fair trial can deprive a victim's family of the justice of a conviction.

Who is at fault in this case, and what is to be done?

Clearly traditional media outlets in the UK who published the story in breach of the order are responsible for putting in peril Grace's family's right to justice.

The 100,000 or so individuals who searched for the name, thereby triggering Google's algorithm for trending topics, have some responsibility.

But New Zealand's Minister of Justice singled out Google for blame and criticism, for its failure to ensure the orders of the courts were respected.

In July, Google apologised for the breach and suspended the Trends Alert subscriber email system that led to the suppressed information being breached.

Last month, it was revealed Google had again breached the name suppression order by twice showing the accused's name in overseas media reports identifying him.

Did Google intentionally flout New Zealand law? I've seen no evidence to suggest this. I have no inside information and know no more about this case than has appeared in the media, but it appears that Google's highly sophisticated, automated service simply acted as it was designed to.

It seems to have been incapable of responding to the combination of factors that the humans in charge of New Zealand's media outlets do, that is; the making of an order, the breaching of the order by irresponsible international media, and the many name searches made by curious individuals.

That unique combination of events poses a real challenge to a global company. Its systems are designed to deploy at a scale that regards the entire population of New Zealand as trivial. So, it is possible to have some sympathy for its plight.

But not much.

The problem of scale is a problem of that platform's own making.

The working title for this session is "*Addressing the Power Asymmetry of the Big Technology Companies*'.

I want to discuss some of the challenges of the new digital economic order. These include challenges to privacy but cut across a range of fields.

We are used to thinking about information asymmetries as one of the market failures that justifies government intervention by regulation.

An information asymmetry is when a consumer does not have sufficient information to make a rational choice about a product or price. It is the basis of most privacy or data protection laws. Every data protection law requires some degree of transparency (if not consent) about the true nature of the transaction in which data is exchanged for goods or services.

But there are other asymmetries. The most glaring I have come to call the "They are one, and we are many" problem.

The "They", in that scenario are the digital monopolies that have taken the "there can be only one" formula for the data economy (one social platform, one search engine, one video platform, one online retailer etc) and have presented a single set of services to a diverse world.

The many are we consumers, nation states, privacy and data protection commissioners, content regulators, competition authorities, electoral commissions.

If we just look at privacy and data protection authorities for a moment, we are over 100 data protection and privacy commissioners working nationally and in-country, providing independent regulation in a patchwork quilt of domestic laws.

It is a challenge for me to meaningfully coordinate domestically with authorities with a shared interest in the values, mores, and cultural settings we are ingesting with our imported technology.

When you multiply the challenge across every jurisdiction with a censor, electoral commission, competition authority, consumer protection authority and online harms agency, the scale of the fragmentation becomes immediately evident. Yet They remain One.

That's the power asymmetry.

And this, in my view, is a unique, and unprecedented problem, and one we are only just beginning to wake up to.

Unprecedented? Not everyone agrees with that. I've seen commentators compare today's digital oligarchs with the Robber Barons of the 19th and early 20th century. Others point to the Microsoft antitrust suits of the 1990's and tell us we've been here before and don't need to reinvent the baby, throw the wheel out with the bathwater, or mix our metaphors to work our way through this.

But we've never been here before. We have companies bigger than countries. Facebook's 'population' of over two billion, none of whom has voting or regulatory rights there.

They move fast and break things, innovate at the speed of fibre optic broadband, deliver fantastic services that improve the lives of billions, and leave regulators in the dust; unable to keep up, unable to match their resources unable to assert effectively that their 'one size fits all product' does not in fact, fit all.

The Christchurch Call

On 15 March this year, a gunman entered two mosques in New Zealand and shot a hundred people, killing 51.

He used automatic weapons of war in his attack. The New Zealand government moved immediately to ban those weapons, as the Australian government did after the tragedy at Port Arthur.

But he also used social media. He live-streamed his attack on a platform that knew of the potential for its service to be used in this way before it launched it. It knew, and failed to take steps to prevent its platform, and audience and technology from being used in that way.

It was predictable and predicted. And the company responsible was silent - confident that the protection afforded by its home jurisdiction would shield it from liability everywhere. We, in New Zealand and Australia, did not vote on, were not consulted on s.230 of the US Communications Decency Act but we feel its effects.

That sections says:

> *"No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."*

The New Zealand government did not move immediately to ban social media – how could it? But did, through the Christchurch call, seek to drive a stake into the ground to delineate some base restrictions on content that are inarguably a legitimate restriction on freedom of expression.

Even before March 15, the topic has been an increasing preoccupation for many regulators.

For example, the twin premises which underlie most social media and interactive platforms developed in the US are “freedom to innovate”, and an almost sanctified version of freedom of expression which elevates free speech beyond many other rights citizens expect to enjoy in western liberal democracies.

The former dominates over the precautionary principle which prevents harms from products and services from occurring prior to those products meeting some regulatory regime or otherwise proving their fitness.

The digital oligarchs argue that the benefits derived from their innovations far outweigh the potential harms, and that they should be left free to let the market decide which ideas fly or die.

But in our society, we also derive great benefits from pharmaceutical products, and air travel, from innovations in genetic engineering. But we do not let entrepreneurs in those fields launch their products without safety testing and regulations to keep consumers safe.

Facebook launched its livestreaming product with the knowledge that it could be used for the purposes the gunman ultimately chose on March 15 and went ahead anyway. They knew the platform could be used to broadcast rape, suicide, murder and other such content. They assured the public that a combination of artificial intelligence, and human moderation would mitigate those risks and allow the public to have the benefits of the technology.

But who examined the biases built into the AI?

The most chilling moment in Facebook’s post Christchurch response (apart from admitting that had the changes they belatedly put in place would have prevented the gunman from streaming his attack) was the statement to US Congress by Facebook's policy director for counter-terrorism who said that its algorithm did not detect the massacre livestream because there was "not enough gore". AI trained on ISIS beheadings did not detect and flag a rapidly firing AR 15.

But the problem is not just limited to the big players. Any tech company can currently create an app such as DeepNude that dehumanises and objectifies women and launch it without screening or preapproval. My colleague from the Philippines is currently battling payday loan apps that have very easy access to credit at

extortionate rates. If you miss a payment, they message everyone in your contacts, and you authorised it!

Data protection laws alone cannot combat these harms. It may be that we need some more agile consumer protection mechanism to allow data protection and privacy authorities to work together with other consumer safety regulators to respond more assertively to the emergence of harmful products in the marketplace.

In this regard I am heartened to see the news, just yesterday, that the ACCC is taking Google to task, under the auspices of fair trade practices, for misleading conduct in relation to the collection of location data.

Perhaps a pre-approval or pre-screening requirement to certify digital products and services would be too cumbersome to administer. But if we are not going to insist on independent ex ante review, we should at the very least impose a duty of care on those who launch products without thinking through the potential for harm and taking all reasonable steps to mitigate those harms.

I am particularly concerned about the co-option, for commercial purposes, of human rights values such as freedom of expression, which reflect the cultural values of the state of origin of the code, and place that value as supreme over what we in our own communities regard as equally important human right such as the right to privacy.

Freedom of expression is a human right. It coexists with other rights that are essential for the development of one's personality. Freedom of thought, freedom of association, the right to privacy. Each of these is fundamental to the maintenance of human dignity.

Corporations do not have personalities to develop, and dignity to preserve, yet they lay claim to freedom of expression because it suits their commercial interests, and the more absolutely it is expressed, the more efficient and less costly it makes their business models.

If freedom of expression trumps privacy, you don't need a costly "right to be forgotten". You can uphold the rights of the online pornographer or incel support group over the privacy right of the betrayed partner in a revenge porn posting.

This exporting of values hard coded into the platforms on which we connect and share and trade and gain our news is increasingly acting as a challenge to traditional concepts of sovereignty, and governments and regulators cannot abandon the field.

There is an incentive on companies to play one nation off against another, one regulator off against another. They claim to want one agreed regulatory model, when what is really needed is for them to comply with the laws and values of the jurisdictions in which they operate. I will return to this point in a moment.

We have seen this approach cause great harm and distress and pain to affected individuals - which we recognise from a framework of the private good of privacy to which those individuals are entitled. But increasingly we are seeing privacy as a public good, a necessary precondition to the survival of some of the fundamental institutions of liberal democracy.

Cambridge Analytica, the Great Hack, Edward Snowden, Brexit, fake news and deep fakes – these are now intrinsic to the chorus of rallying cries to recalibrate the balance between the freedom of these platforms to operate, and sensible regulation to preserve our democratic institutions.

We're at a global tipping point of not continuing to be passive takers of technology that increasingly takes control away from the individual.

ACCC Digital Platforms Inquiry

In June this year, the Australian Competition and Consumer Commission, following the lead of counterparts in the UK, Singapore and elsewhere released its thorough Digital Platforms Inquiry report.

The report looked specifically at the impact of digital platforms on consumers, businesses using platforms to advertise to and reach customers, and news media businesses that use the platforms to disseminate their content.

Facebook

Instead, Facebook said some ACCC's recommendations would "*make targeted advertising practically unworkable in Australia".*

It would put Australia *"out of step with other countries such as Singapore and the European Union."* Its submission said:

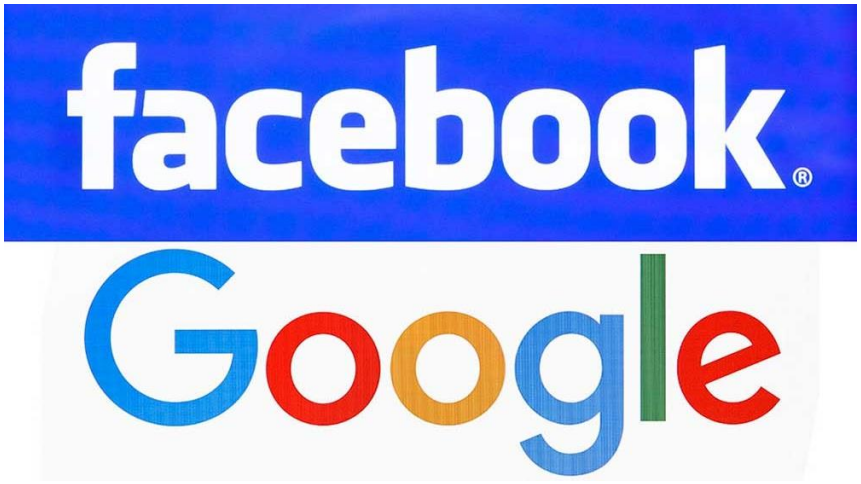
> *"To ensure proper alignment and consistency, the aim should be to stick as closely as possible to the GDPR wording."*

But why should Australia have *"alignment and consistency"* to suit Facebook? Why should New Zealand have "*alignment and consistency"* to suit Facebook?

Digital platforms need to adapt to the jurisdictions in which they operate - not the other way around.

And maybe some kinds of *"targeted advertising*" should be *"practically unworkable"* – especially if they are deeply intrusive, there's no meaningful consent and there's no way to opt out.

We know that Facebook offers thousands of different market segmentations that advertisers can target. These can be explicitly racist or divisive, such as allowing advertisers to target self-declared or inferred "Jew-haters', or through a myriad of proxies facilitated through thousands of seemingly innocent data points.



We know that Google on its YouTube platform has been nudging viewers along pathways towards more extreme content.

These assumptions and assignments of what we want to view or read online are having an increasingly toxic effect on our social and democratic institutions, and our discourse.

What's that got to do with privacy? It's all based on our data - obtained under mostly false pretences, deceptive conduct or half true declarations of purpose buried in a thesis-length legalese privacy policy.

This is an unequivocal call for more regulation, spanning, for example, antitrust consumer rights, anti-competitive practices, privacy, and electoral integrity.

Click to consent

One of the ways to correct the information asymmetries that plague the online environment is by a more focused attention on transparency. Not consent necessarily, but at least an open, clear and honest disclosure of the data consequences of any given engagement.

Internationally, the days of click to consent are numbered because it is not meaningful consent.

New Zealand's Chief Justice in her lecture last year commemorating the first New Zealand Privacy Commissioner, Sir Bruce Slane, said:

“There is good reason for proceeding with caution when weighing the significance to be given to consent when assessing whether the individual expected privacy or had waived it.

These are standard contracts people must agree to if they are to access services, sometimes essential services.

Most do not read the full content of any such contract. That is especially so with online service providers.

Although the privacy policy must be agreed to before services can be accessed, acceptance is easy — simply click on the accept button.”

When the Privacy Bill comes into effect in 2020, it has clear and explicit application to all agencies doing business in New Zealand, whether they have a physical base here or not.

The digital giants are addressing this issue in other parts of the world. It is important that I give clear notice of the law they are expected to comply with here, and how I apply it. I’ve done so in a blog post recently in which I have spelled out how I see the transparency obligation.

IAPP **ANZ SUMMIT 2019**

The new Privacy Act (due in force in July next year) will have an explicit extraterritorial application and will give me the power to issue compliance notices to business to improve the digital environment for consumers, whether companies are based in New Zealand or just doing business there.

I’ll be able to deploy compliance notices for:

- serious breaches that the agency is unwilling to address.
- systemic or repeat breaches where no progress is made.
- situations which require a middle person in the enforcement process, using up additional time and resources.

On receiving one, the agency must comply as soon as possible or:

- apply to vary or cancel the order by persuading my office that you've already complied or are in the process of complying.
- appeal the notice within 15 working days.

Failure to comply means my office can take enforcement proceedings in the Human Rights Review Tribunal.

The agency's only defence will be if it believes the notice has been fully complied with.

These will be welcome additions to the light-handed regulatory approach New Zealand has had for the last 26 years but will not be enough to defeat the problem I outlined at the outset.

Let me give you an indication of why.

Viagogo

The NZ Commerce Commission, which administers the Fair Trading Act last year commenced enforcement action against Viagogo. An online company based in Switzerland, with no physical presence in New Zealand. That Act has explicit extraterritorial reach.

Viagogo facilitates scalping, the sale of fake tickets, and also allegedly engages in deceptive conduct about how many tickets were left for an event and how fast they were selling.

New Zealand's Commerce Commission has so far spent $1.2 million pursuing the company just to have the High Court decide not to issue an interim injunction against the company. This is just for one case, against one company.

It underlines again the asymmetry in the power dynamic between an offshore tech company like Viagogo and a domestic regulator.

End note

Small countries like New Zealand need to ensure that they are internally unified against the threats presented by unscrupulous digital operators, so that whether the threat presents in a context of election integrity, harmful content, privacy or consumers' rights, we are working as one for the people we represent.

And even more importantly, we need to combine internationally to push back against the one-sided offering we get from the companies that profit from our populations' data.

One of the lessons from Christchurch is that when we join together and present the irrefutable moral right, it can force industry to act, and that even though we represent only a fraction of the user base of those platforms, we can make our voice count in very real and practical ways.

But it mustn't take another terrorist atrocity, or corrupted election or referendum, or Myanmar genocide to get and hold their attention.