Consumer Analytica: New Zealand Consumer Law Application to International Developments in Privacy and Use of Data

Sarah Keene and Troy Pilkington [1]
11 August 2018

1. In April 2018, Mark Zuckerberg, founder and CEO of Facebook, testified before the US Congress, in response to revelations about Cambridge Analytica accessing the personal information of over 80 million Facebook users (including over 60,000 of New Zealanders).[2] When asked whether the use of data by online platforms ought to be better regulated, Zuckerberg responded "if it's the right regulation, then yes".[3]

2. Mr Zuckerberg's answer lends itself to an obvious follow-up: What is the right regulation? How do governments best harness the benefits of big data and artificial intelligence, while simultaneously protecting consumers from the risks which inherently accompany this way of doing business?

3. New Zealand is not immune from these challenges. New Zealand is publicly predicted to see a big take-off in the use of artificial intelligence in the next 3-5 years, with the potential to see it adopted on a mass scale throughout all businesses within 20 years.[4] The use of artificial intelligence is set to grow at a similar rate.[5]

4. While the impacts of this "fourth industrial revolution" are wide-ranging,[6] this paper refers to regulatory challenges in two specific arenas:

   (a) The collection and use of consumer data. This refers to how businesses collect data from consumers, store it and then use it to inform their decision making processes and product offerings (hereon referred to as **"Big Data"**); and

   (b) The use of artificial intelligence. This refers to the use of computers to perform tasks which, in the past, required human intelligence to complete (hereon referred to as "**Artificial Intelligence**" or "**AI**"). While the use of Artificial Intelligence spans numerous business functions, this paper is concerned with the automation of consumer-facing business functions (computers replacing call-centre personnel, for example).

5. This paper considers the regulation of Big Data and Artificial Intelligence in the consumer-law space. It first sets out an overview of the risks and benefits of Big Data and Artificial Intelligence to consumers. It then considers four particular ways in which Big Data, Artificial Intelligence and consumer law are likely to interact with each other in the coming years.

---

[1] Sarah Keene is a Competition, Regulatory and Consumer Law Partner and the Chair of Russell McVeagh's Public, Regulatory and Competition Law Practice (https://www.russellmcveagh.com/our-people/sarah-keene); Troy Pilkington is also a Competition, Regulatory and Consumer Law Partner at Russell McVeagh (https://www.russellmcveagh.com/our-people/troy-pilkington). The authors thank Chris Brunt, Graduate in Competition and Consumer Law, for his work on this supporting paper.

[2] https://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=12028791

[3] https://techcrunch.com/story/zuckerberg-testifies-at-congressional-hearings/

[4] https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=12039307

[5] https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=11678678

[6] The term "Fourth Industrial Revolution" refers to a digital revolution characterised by "a fusion of technologies that [blurs] the lines between the physical, digital, and biological spheres"; https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

THE IMPERATIVE OF A BALANCED APPROACH TO AI OR BIG DATA REGULATION

6. Regulation of Big Data and Artificial Intelligence in the consumer-law space requires a balancing of potential risks and rewards. The consumer welfare enhancing effects of the use of Big Data and Artificial Intelligence are undisputed and wide-ranging. They include better targeting of healthcare to patients, improved equal access to employment and heightened access to credit using non-traditional methods.[7]

7. However, Big Data and Artificial Intelligence also pose a number of key challenges in the consumer-law space. In relation to Big Data, these challenges include:

   (a) Use of inaccurate data. If a business is using consumer data for decision-making, it is imperative that this data is accurate. Inaccurate or incomplete data can cause businesses to make ill-informed consumer decisions. This is particularly problematic if incomplete data reinforces existing biases against certain forms of consumer.

   (b) Data security. This refers to the challenge of protecting customer information from data breaches. Major data breaches are an increasing problem, especially with increased state-sponsored cyber engagement from many countries globally.[8] The adequacy of steps taken by organisations to keep consumer data safe is a key concern, and is dealt with directly by the New Zealand Privacy Act.[9]

8. Artificial Intelligence also poses a number of key challenges to consumers, including:

   (a) Unsatisfactory or discriminatory algorithmic decision-making. This challenge refers to the risk that, when algorithms replace human decision-making processes, there is potential for them to discriminate against certain forms of consumer and/or mislead customers. This risk is exacerbated by the inability to understand, in human terms, algorithmic decision-making processes, as discussed at (b).

   (b) Lack of accountability for Artificial Intelligence decision-making. AI is capable of programming itself. By the Federal Trade Commission's (**"FTC"**) own admission, it may not be possible to "interrogate" an AI system or understand why it is behaving in a certain way.[10]

   These self-learning algorithms are best understood as "black boxes" - humans can give the algorithm access to input data and interpret the decisions that it outputs, but cannot understand the processes by which it arrives at the output.[11] If regulators, and even the architects, cannot understand the process by which an algorithm arrives at a decision, these self-learning algorithms become very difficult to regulate.

---

[7] Federal Trade Commission "Big Data, a Tool for Inclusion or Exclusion", found here.

[8] https://securityintelligence.com/news/report-shows-increase-in-data-breaches-in-the-first-half-of-2017/

[9] Principle 5 of the NZ Privacy Act requires agencies holding personal information to ensure that the information is protected by such security safeguards as is reasonable in the circumstances.

[10] Terrell McSweeny (FTC Commissioner) "Data & Algorithms: What do they mean for competition and consumer protection enforcement?" Presented 11 April 2018. Found here.

[11] http://bigthink.com/21st-century-spirituality/black-box-ai

SPECIFIC INTERACTIONS OF BIG DATA, AI AND CONSUMER LAW

9. The remainder of this paper deals with four particular examples of how Big Data or AI are likely to interact with consumer law in the future:

   (a) Fair Trading Act breaches by digital platforms like Facebook. The US FTC have brought charges against digital platforms (Snapchat and Twitter, for example) under the equivalent of the New Zealand Fair Trading Act's (**"FTA"**) prohibition of misleading and deceptive conduct. This section considers these charges, and whether the New Zealand Commerce Commission (**"NZCC"**) could bring FTA charges against digital platforms in New Zealand in a similar manner.

   (b) Unfair contract terms and the collection of Big Data. Businesses often collect consumer data in the course of non-negotiable, 'take-it or leave-it' contracts (broadband contracts where customers have no choice but to give the provider access to their browsing data, for example). Given the increasing value of data to businesses and the increasing potential for its misuse, businesses that acquire data in this way may breach unfair contract legislation.

   (c) Misrepresentations made in the course of sharing data. As the use of open-data solutions (open banking, for example) increases, businesses will inevitably be involved in using other's data more frequently. This section explores potential FTA risks for businesses that are transferring their data to other businesses and/or using data and information that has been transferred to them.

   (d) Strict Liability for creators of misleading or deceptive artificial intelligence. Traditionally, employers have been held accountable for the misleading or deceptive conduct of their employees (who are treated as the business's agents). As consumer-facing personnel are increasingly replaced by computers, this section deals with the FTA implications of the potential for artificial intelligence to mislead consumers.

FAIR TRADING ACT-TYPE ACTIONS AGAINST DIGITAL PLATFORMS

10. Section 9 of the FTA provides that:

> No person shall, in trade, engage in conduct that is misleading or deceptive or is likely to mislead or deceive.

11. Section 5 of the United States Federal Trade Commission Act ("**FTCA**") is similar, prohibiting "unfair or deceptive practices in or affecting commerce."

12. There is potential for a business' use of Big Data, in relation to consumers, to amount to misleading and deceptive conduct. There have been no charges of this kind laid against New Zealand businesses under the FTA. However, there have been a number analogous actions brought by the Federal Trade Commission ("**FTC**") under section 5 of the FTCA.

13. The FTC have laid these charges in a range of circumstances, as described below:

   (a) If a business violates a promise to consumers relating to its use of their data. For example, if a business promises to safeguard a customer's personal information from use or theft by third parties, and then fails to do so.

(b) A failure to disclose material information to the consumer regarding how data is used. For example, the FTC has previously laid charges against a credit card company which adjusted the amount of credit available to customers depending on the items purchased with their credit cards. Available credit was reduced for customers who used their card at pawn shops or on marriage counselling. Customers were not informed of the business monitoring their spending.[12]

(c) A business which sells customer data to a purchaser when it knows - or ought to know - that the purchaser intends to use the data for fraudulent purposes. For example, an organisation which sells data to identity thieves when it knows, or ought to know, that the purchasers are identity thieves.

14. The FTC has also brought a number of cases against digital platforms for their treatment of user information:

(a) In 2014, the FTC charged Snapchat under section 5 of the FTCA for:[13]

(i) misleading its 191 million daily users[14] about whether their messages were deleted after they had been read (Snapchat told customers that it immediately deleted these messages, when it was taking no such action);

(ii) failing to secure user's personal information, causing the details of 4.6 million users to be stolen in a security breach; and

(iii) deceiving customers over the amount of personal data it collected.

Snapchat eventually settled these charges with the FTC for an undisclosed sum.

(b) In 2010, the FTC also brought charges against Twitter for failing to secure its user's personal information. This allowed hackers to access private user information, and to send out "phony" tweets from various accounts (including then President-elect Barack Obama's account).[15]

15. The current guidance provided on the NZCC's website frames misleading and deceptive conduct in terms of false representations made to customers as part of their advertising or sales functions.[16] There is no mention of the misuse of data. However, given that the use of Big Data is set to continue its rapid growth in the coming years, it is likely that regulators like the NZCC will, at some point in the future, look to utilise all legislative tools in their 'toolkit' to prevent data misuse from occurring.

Case Study - Cambridge Analytica

16. A 2018 paper found that Facebook's standard terms of use:[17]

[12] *FTC v Compucredit Corporation* (2008), found here.

[13] https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were

[14] https://www.statista.com/chart/7951/snapchat-user-growth/

[15] https://www.ftc.gov/news-events/press-releases/2010/06/twitter-settles-charges-it-failed-protect-consumers-personal

[16] http://www.comcom.govt.nz/fair-trading/fair-trading-act-fact-sheets/what-is-the-fair-trading-act/

[17] Catalina Goanta "Facebook's Data Sharing Practices under Unfair Competition Law" (June 2018). Retrieved from https://ttlfnews.wordpress.com/2018/06/08/facebooks-data-sharing-practices-under-unfair-competition-law/

(a) contain only a vague description about the transfer of customer data to third parties, but remains silent as to how or with whom this transfer will take place; and

(b) make no reference to the extent to which Facebook will access a user's friends' data and, equally, to what extent a user's data is vulnerable to collection by virtue of their friends' inadequate privacy settings. This was how Cambridge Analytica accessed the personal information of nearly 80 million users between 2010 and 2015.

17. The scope of the FTC's current investigation into Facebook relating to Cambridge Analytica is not publicly available yet, and there is no indication of whether it is likely to include a charge of "misleading and deceptive conduct" under the FTCA.[18] However, when more information is released, and subject to the relevant limitation periods, it is possible that the NZCC could consider its position, given that the data of over 60,000 New Zealanders was accessed by Cambridge Analytica.

18. The New Zealand courts tend to generally adopt a consumer-friendly approach to the "overall impression" of statements made.[19] While it is currently unclear whether, and if so in what respect, Facebook made statements that gave consumers an overall impression about the transferability of their data, this is not a prosecution that is conceptually outside of the NZCC's framework of options.

UNFAIR CONTRACT TERMS AND THE COLLECTION OF BIG DATA

19. In addition to the misleading and deceptive conduct prohibition, the prohibition on unfair contract terms in standard form consumer contracts (section 26A of the FTA) also plays an important role in consumer protection with respect to Big Data.

20. The NZCC will deem a contract term unfair if:[20]

(a) it is part of a standard form consumer contract; and

(b) it has all of the following attributes:

(i) it causes a significant imbalance in the parties' rights and obligations arising under the contract;

(ii) it is not reasonably necessary to protect the legitimate interests of the party who would be advantaged by it; and

(iii) it would cause detriment (whether financial or otherwise) to a party if it were applied, enforced or relied on.

21. This section considers whether contract terms between businesses and consumers pertaining to the collection and use of personal information could be considered unfair and, if so, the likelihood of the NZCC using this legislative tool to regulate the use of Big Data in the future.

---

[18] https://www.theguardian.com/technology/2018/mar/26/facebook-data-privacy-cambridge-analytica-investigation-ftc-latest

[19] *Godfrey Hirst NZ Ltd v Cavalier Bremworth Ltd* [2014] 3 NZLR 611.

[20] Fair Trading Act 1986, s 46L(1).

22. Consumer contracts for everyday products and services (such as banking, telecommunications and public transport) often give the organisations providing these essential services access to large quantities of data. For example, when a consumer makes an agreement with a social media platform, they give the platform access to data about their friendships, activities and interests.

23. Michiel Rhoen describes these contracts as "privacy contracts". They are not primarily concerned with data - the consumer is not directly selling their personal information to a business. Rather, the collection of data is incidental to the primary purpose of the arrangement (i.e. a business provides a customer social media services, and the customer incidentally consents to the business collecting and using its browsing data).

24. These contracts are characterised by their data-related terms being non-negotiable (i.e. part of a standard form consumer contract), and their underlying subject matter often being a necessity good or service for consumers. Accordingly, consumers are often left with no choice but to give businesses access to their data, in order to acquire essential goods and services.

25. With respect to the other requirements for a contract term to be considered unfair (as outlined at 20(b)):

    (a) Imbalance in the parties' rights. As Big Data analytics continues to 'boom', the value of customer information will undoubtedly continue to increase. Extracting data from customers in circumstances where they are unable to negotiate a fair price for their information could give rise to a significant imbalance in the parties' rights;

    (b) Not reasonably necessary to protect business' legitimate interests. If a business can show that it has a legitimate reason to collect consumer information as part of a contract (for example, a telephone company recording the number of calling minutes a consumer uses if it bills on a per minute basis), then the term may not be considered unfair. However, if the collection of data is not necessary for the business to function, there may be more than one view on whether it is "reasonably necessary to protect business' legitimate interests."

    (c) Detriment caused to the consumer. Given the increasing importance of Big Data analytics in the way that businesses interact with consumers, it is plausible that the collection of valuable customer information in a non-negotiable fashion could be detrimental to the consumer.

26. As with the misleading and deceptive conduct provisions of the FTA, the NZCC is yet to utilise unfair contract legislation to regulate Big Data. However, overseas competition authorities have shown a recent willingness to do this. In particular, the Italian Competition Authority (**"ICA"**) has brought a number of cases in this space recently:

    (a) In 2016, the ICA found that WhatsApp effectively forced its users to accept new terms of service, by inducing existing users into believing that "without granting such consent they would not have been able to use the service anymore."[21] These new terms included provisions that permitted WhatsApp to share its user's personal details with Facebook. The ICA fined WhatsApp NZ$5.2 million.

[21] http://www.agcm.it/en/newsroom/press-releases/2380-whatsapp-fined-for-3-million-euro-for-having-forced-its-users-to-share-their-personal-data-with-facebook.html

(b) In April 2018, the ICA launched an investigation into Facebook's Big Data practices, specifically alleging that:

(i) Facebook's default settings (i.e. a pre-selected box) provided for the transfer of personal data to third parties, every time the user interacted with the third parties' Facebook application; and

(ii) Facebook did not adequately inform their users of their option to 'opt out' of this agreement to transfer their personal data to third parties.

The ICA is investigating whether these commercial terms are unfair, and whether Facebook "exercises undue influence" on its users, who wish to continue using its online platform, to consent to unreasonable use and transfer of their data.

27. Given that the ability of organisations to use data analytics to derive insights from personal information is set to increase in the coming years, organisations are likely to be increasingly incentivised to collect, use (and in some cases, sell) personal information by any means possible, including non-negotiable, "take it or leave it" terms within consumer contracts.

Unconscionable Conduct

28. In addition to its prohibition on unfair contract terms, Australia also prohibits businesses from engaging in 'unconscionable conduct'.[22] While New Zealand has previously considered implementing a prohibition on unconscionable conduct, it is not currently part of our FTA framework.

29. However, the need for a stronger punitive measure against this sort of behaviour may become apparent in the coming years, as the value and use of Big Data increases. Accordingly, Parliament may see seek to revisit whether a prohibition of unconscionable conduct ought to be added to the NZCC's enforcement toolkit.

MISREPRESENTATIONS MADE IN THE COURSE OF SHARING DATA

30. The third potential consumer law risk for businesses using Big Data arises in the context of businesses transferring consumer data between themselves. As discussed **above**, businesses who mislead their customers as to how their personal information is being used (i.e. if it is being sold to third parties without the customer's informed consent) are potentially in breach of the FTA.

31. However, businesses transferring data between themselves may also potentially expose themselves to other liability under the FTA's prohibition on misleading and deceptive conduct.

32. An increased level of shared data between businesses is another symptom of the '4th industrial revolution'. This has particularly manifested itself in arrangements between businesses in the same industry to share data between themselves (open banking solutions, for example) (collectively referred to as "**Open Data Solutions**").

[22] https://www.accc.gov.au/business/treating-customers-fairly/unfair-business-practices#unconscionable-conduct

33. This move towards Open Data Solutions has been precipitated by reforms like the Australian 'Consumer Data Right', which aims to give consumers the right to "control their data, including who can have it and who can use it".[23]

34. While the Australian Treasury anticipates that Open Data Solutions could be rolled out across multiple sectors in the coming years (energy, telecommunications), the banking sector is the first industry where the implications of an open approach to data sharing are being fully considered.[24]

35. Open banking involves giving customers a right to direct information that they have already shared with their bank (i.e. their income, expenditure) to be shared with other businesses that they trust (a mortgage broker they want to borrow from, for example).

36. While, unlike Australia, the New Zealand government is not yet contemplating a legislated open banking solution, a number of private open banking pilots have already taken place in NZ. For example,[25]

    (a) Payments NZ is an open banking pilot project involving ASB, BNZ, Paymark, Datacom, TradeMe and Westpac.

    (b) Jude is an open banking solution which will allow consumers to access all of their bank accounts on a single platform, making it "possible for people to seamlessly operate accounts and services from different banks through a single portal."[26]

37. While clearly transformational for consumers, open banking solutions (and Open Data Solutions more generally) will necessitate businesses transferring an unprecedented quantity of data between one another.

38. There is potential for this transfer of data to amount to misleading or deceptive conduct if, for example:

    (a) there is an error in the data transferred from one business to another (whether intentional or because of a technical error); or

    (b) the context in which the data was collected in is not properly communicated to its recipient, leading to its misinterpretation.

39. This risk is exacerbated by the fact that the transferors and recipients of shared data will often be competitors (major retail banks, for example). Accordingly, any confusion that the transferor can cause for the recipient will be to its commercial advantage.

40. The FTA could be used in these circumstances in two different ways:

    (a) A civil claim for misleading and deceptive conduct, brought by the data recipient against the transferor. The FTA generally governs business-to-business (**"B2B"**) relationships by providing a legislative basis for parties to bring civil claims against each other. The NZCC does not generally intervene in FTA disputes between two businesses. The recipient of misleading and deceptive information will only be able

---

[23] https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf at v.
[24] https://static.treasury.gov.au/uploads/sites/1/2018/02/Review-into-Open-Banking-_For-web-1.pdf.
[25] https://www.stuff.co.nz/business/102524114/open-banking-pilot-begins-in-new-zealand
[26] https://www.stuff.co.nz/business/102524114/open-banking-pilot-begins-in-new-zealand

to bring a civil FTA claim against the transferor if the parties have not contracted out of the FTA in their data-sharing agreement.[27]

(b) Where misleading and deceptive conduct by data transferors is causing significant dysfunction, to the ultimate detriment of consumers, in:

(i) the market which the data transferors and recipients operate in; or

(ii) a downstream market,

the NZCC may consider there to be sufficient grounds to intervene, and bring FTA action for misleading and deceptive behaviour against parties allegedly behaving unlawfully. The NZCC regularly enforces the FTA in a manner that benefits competitors, in the interests of delivering markets with a level and transparent playing field.

STRICT LIABILITY FOR CREATORS OF MISLEADING OR DECEPTIVE ARTIFICIAL INTELLIGENCE

41. The final part of this paper concerns situations where a computer, which has replaced a human in a consumer-interfacing role, acts in a misleading and deceptive manner.

42. For example, if a business replaces its call-centre personnel with computers, and one of these computers misleads or deceives a caller, the computer's algorithm has caused the company to breach the FTA.

43. Consumer-interfacing robots misleading consumers presents a material risk for organisations that deploy this technology. A 2015 Stanford Report concluded that robots deceiving customers was an "inevitability", especially given the often complex nature of the interactions between businesses and consumers:[28]

> A modest amount of inaccuracy is allowable, if not encouraged, under general principles of marketing and the messiness of human interaction. Many robots that end up misleading people might simply be engaged in trade puffery or common data analytics, similar to how a salesperson relies upon context and cues to tailor a strategy to best close the deal.

44. While the potential for consumers to be misled by computers, bringing consumer-law enforcement action against a computer is problematic, not least because its decision-making processes will often be indecipherable in human terms.

45. Complex consumer-facing algorithms are not just a series of *'if-then statements'*.[29] Indeed, FTA enforcement relating to the actions of a consumer-facing computer is hghly unlikely to arise from a line of code which says *"if the customer says X, lie to them about Y"* (indeed that may well be a form of fraud and prosecuted accordingly). Rather, Artificial Intelligence is often 'self-learning', meaning that it is conceivable that a computer could teach itself to mislead or deceive consumers. This algorithmic decision-making:

---

[27] Businesses are able to contract out of the FTA in the context of B2B relationships, provided that it is fair and reasonable for them to do so. See http://www.comcom.govt.nz/fair-trading/fair-trading-act-fact-sheets/contracting-out-of-the-fair-trading-act/.

[28] http://www.werobot2015.org/wp-content/uploads/2015/04/Hartzog-Unfair-Deceptive-Robots.pdf

[29] This analysis is based on MIT Technology Review article titled *'The dark secret at the heart of AI'*, found here.

(a) may not be the result of direct instruction given to the computer by its owner; and

(b) may not be decipherable in human terms. It may not be easy to identify how the algorithm mislead the consumer, as the computer may be incapable of explaining its decision making process to its human owner.

46. In these circumstances, the enforcement role of a consumer law regulator is simply to prove, on the balance of probabilities, that misleading and deceptive conduct has taken place. Defending the action on grounds of lack of intention or mistake becomes nearly possible.

47. In the same way that employers are still held liable for misleading and deceptive conduct by their employees, international regulators have argued that organisations should be held responsible for representations that their algorithms make, even if humans do not initiate (or even understand) these behaviours.

48. European Commissioner Margrethe Vestager recently articulated this point of view (albeit in a competition law context):[30]

> What businesses can and must do is to ensure compliance by design.
> …
> What businesses need to know is that when they decide to use an automated system, they will be held responsible for what it does. So they had better know how that system works.

49. The strict liability nature of the FTA offences makes this approach even more likely to prevail in the New Zealand consumer law context.

50. However, enforcement decisions will need to be taken intelligently, and the NZCC should publish guidelines regarding its regulation of AI, which set out its enforcement processes and benchmarks as they relate to consumer-interfacing computers. Over-enforcement could have a potentially stifling effect on innovation and technological development in this space. The threat of Artificial Intelligence causing its owners to breach the FTA (despite no intentional wrongdoing on their behalf) is likely to disincentivise investment in consumer interfacing Artificial Intelligence in the first instance.

CONCLUSION

51. The use of Big Data and Artificial Intelligence is likely to be a considerable disruptive force in consumer law over the coming years. These new technologies have the potential to make significant improvements to business efficiency, and to deliver real value to consumers across any number of industries.

52. However, they also pose a number material risks to consumers. These risks range from misleading behaviour on the part of consumer-interfacing robots, to the transfer of consumer's personal information from one platform to another without their consent. New Zealand consumer law has an important role to play in mitigating these risks, but lawmakers and regulators must also be minded not to stifle innovation by taking an over-aggressive approach to regulation and enforcement in this space.

---

[30] Politico: *When When Margrethe Vestager takes antitrust battle to robots*, available here.

53. Further to this, as businesses and consumers attempt to navigate how these new innovations interact with New Zealand's existing consumer law framework (and any potential changes to the law in the coming years), comprehensive communication from the NZCC and other regulators as to their likely enforcement approach will be vital. As part of this process, it will be important that lawmakers and regulators establish an ongoing dialogue with businesses and consumers about the risks and benefits of particular technologies, practices and regulatory approaches.

Your contacts

Sarah Keene
Partner

Sarah.Keene@russellmcveagh.com
DDI: +64 9 367 8133 |

Troy Pilkington
Partner

Troy.Pilkington@russellmcveagh.com
DDI: +64 9 367 8108 |