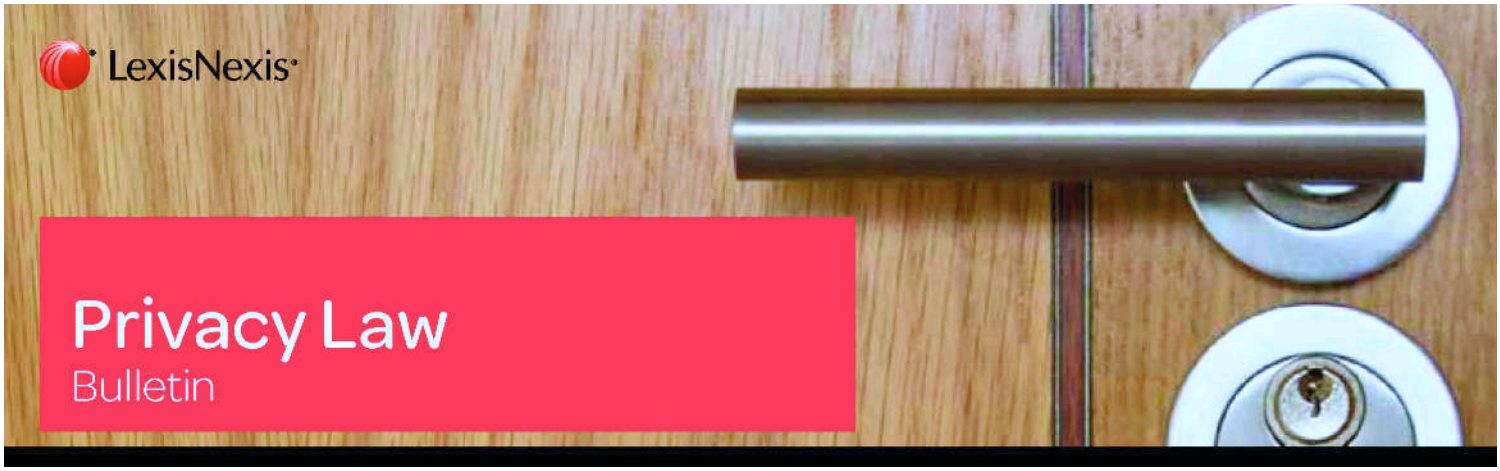

Privacy Law Bulletin

2018 . Vol 15 No 5

Contents

Information contained in this newsletter is current as at July 2018

LexisNexis Butterworths

Privacy Law
Bulletin

Securing the Internet of Things: a global overview of a global challenge

Albert Yuen *and* ***Erica Chan*** *GILBERT + TOBIN*

Introduction

Last year, Internet of Things (IoT) devices officially began to outnumber the world's human population.[1] While connecting devices to the internet is not a new thing, the scale of the IoT is changing our relationship with data. In addition, greater attention has been given recently to the development and use of IoT devices and services to ensure they consider privacy and security issues. However, regulatory approaches and standards relating to privacy and security issues of IoT devices have varied. With Australia's new mandatory data breach regime[2] and the European Union's (EU) new and border-crossing General Data Protection Regulation (GDPR)[3] having come into effect recently, now is an important time for Australian companies to assess their strategy around privacy, security, the IoT and the global position on the IoT.

Key takeaways

- The proliferation of IoT devices and service adoption by corporates and consumers have heightened concerns around consumer privacy and security. As there is increased use of IoT data, corporations face challenges in managing, transmitting and sorting these huge volumes of data securely as well as meeting privacy challenges raised by IoT devices, including where data is collected in a "passive" way (eg, through monitoring devices such as mobile apps).
- While Australia principally regulates the IoT through Australian privacy laws, consumer laws, and industry-specific laws and codes for IoT providers, there aren't any specific IoT-focused regulatory regimes. This is generally similar to the IoT regulatory approach in major jurisdictions worldwide.
- There are many initiatives underway in Australia and overseas to formulate guidelines, industry codes and areas of good practice for the supply and use of the IoT and other data-driven services. Industry-led initiatives within Australia and globally have provided good frameworks for understanding the best approach to how IoT regulation, principles, guides and codes are developing. As such, this article aims to take a global stocktake of key markets in how they deal with IoT privacy and security issues. All companies, especially those looking to operate internationally, should consider the increasing consumer concern, different regulatory regimes and industry initiatives when developing their IoT privacy and security strategies.

Key IoT privacy and security challenges

What is the Internet of Things?

The IoT can be defined simply as "the networking of physical objects connecting through to the Internet"[4] and each other. However, this definition belies the increasing complexity and impact of the IoT. We can find a more powerful metaphor from Kevin Ashton, known as the "father of IoT", who has compared the IoT to the human nervous system.[5]

It's a surprisingly apt comparison. Firstly, it reflects the incredible scale of the IoT and its connections: research firm Gartner predicts that by 2020, we will have approximately 20.5 billion IoT devices.[6] Secondly, it gives us a useful perspective of the IoT in practice. After all, like our own nervous systems, IoT devices are constantly collecting and transmitting information to be used in analysis and decision-making.[7]

Lastly, just like our nervous systems, the IoT is open to serious attack. The connectivity and number of IoT devices mean that breaching the security of a single device can infect every single other device in the network, allowing criminals to launch distributed denial-of-service (DDoS) attacks to steal data or bring down online services.[8]

The power and disruptive promise of the IoT is the exponential scale of its data. As the number of devices capable of internet connectivity increase, and as IoT device manufacturing, connectivity and data costs are reduced, there is an unprecedented scalability of IoT solutions. However, the proliferation of data collection, storage and transmission and use from the IoT also

raises increased concern about privacy and security risks, as well as consumer confidence around the IoT design process. Together, these elements of the IoT showcase the primary challenges that our increasingly connected world poses: protecting privacy and securing the IoT.

The challenge of consumer privacy

The everyday use of IoT devices is inescapably eroding individual privacy. To demonstrate this, journalist Kashmir Hill recently converted her apartment into a "smart home" to run a privacy experiment with her colleague Surya Mattu.[9] Hill bought a number of IoT devices, including a smart bed, a smart television, smart lights, and even a smart coffee maker. Mattu used a router to capture all of Hill's IoT device activity. Only a few months of monitoring revealed a treasure trove of data. For example, Mattu could track exactly when family members were going to bed and when they left the apartment through their smart lights and Amazon Echo. Mattu also found that Hill's smart television was collecting second-by-second information about everything the family watched, from commercials to DVDs, and selling that data to advertisers.

Hill's article describing her IoT and privacy experiment touched a nerve. In the flood of commentary following it, many raised concerns that none of this information is necessarily recognised as "personal information" and protected by privacy laws. That's certainly true in Australia, where the Full Federal Court held last year that metadata — even location data allowing companies to track where individuals live and how they go to work — is not necessarily personal information unless it passes the threshold question of whether it is directly "about" an individual.[10] Companies providing or utilising IoT devices or services will need to be fully compliant with the law (including managing Australian Consumer Law (ACL) issues around any defective IoT devices, with indications that Australian regulatory bodies are determined to ensure consumer laws keep pace with developing technologies such as the IoT)[11] and need to carefully manage these risks, including running afoul of consumer ire and public activism.

The challenge of security

The second challenge of the IoT is security. IoT devices often have many vulnerabilities, including problematic infrastructure, improper authentication mechanisms and lack of encryption, resulting in the well-founded fear that IoT devices are the greatest threat to individual security today.[12]

Companies face another level of complication. In her experiment, Hill ran into an unforeseen problem: compatibility. To run all of her devices, she had to download 14 different applications, and not all of her IoT devices were compatible with each other.

For Hill, this was frustrating. But at a business level, it means that companies that manufacture, supply, or use IoT devices are finding themselves in an increasingly complicated supply chain with multiple parties, ranging from data analytics providers to third-party software developers.

The first wave of IoT commercialisation saw vendors trying to provide end-to-end solutions to cut down on such complexity. However, the consumer-driven market has led to more fractured, mix-and-match, and multi-vendor approaches. For our clients, we have seen that these approaches provide both customisation and challenges, including:

- determining data breach liability and response management between multiple vendors
- managing clashing privacy policies and data practices in coordinating critical responses to data breaches
- the reality that the privacy and data security of the whole supply chain is only as strong as its weakest link, which may be a subcontractor in another jurisdiction

Such challenges show that there needs to be renewed focus on user preferences and the IoT design process relating to a user's awareness of the collection, processing, use and transmission of information (including potential personal information) in IoT solutions.[13]

The global IoT privacy and security landscape

Faced with both the inherent insecurity of IoT devices and the complex commercial relationships surrounding them, it is no wonder that Gartner has predicted that worldwide spending on securing the IoT will reach $1.5 billion this year.[14] Such expenditure is a sign of how the landscape has shifted to meet the monumental privacy and security challenges of the IoT. Only a short time ago, it was a common lament that consumers either were not aware of, or simply did not care about, how using technology affected their privacy. That is no longer the case. The Economist Intelligence Unit recently released a report showing that 92% of global consumers surveyed wanted to control the scope of automatic collection of personal information and 92% wanted heavy punishments for companies that violated their privacy.[15] Recent and well-publicised privacy scandals involving Facebook and Cambridge Analytica have certainly contributed to such views.

In response, governments and industry organisations around the world are taking a number of different approaches.

Australia

Australia currently has no specific legislation which specifically regulates the IoT. Instead, the IoT in Australia is governed under privacy legislation (as it relates to the collection, storage, use and transmission of personal information or "sensitive information" of individuals), and the ACL (as it relates to the use of IoT products and services for domestic consumer purposes).[16] The use of IoT devices in certain industries may also fall under regulation, such as the Telecommunications (Interception and Access) Act 1979 (Cth) requiring telecommunications companies to retain certain data for 2 years. The Office of the Australian Information Commissioner (OAIC) has also recently published guidance to assist organisations to identify and take steps to address privacy issues related to data analytics, including the use of the IoT.[17]

The responsibility for direct regulation of the IoT seems to have shifted to industry, with the IoT Alliance Australia (IoTAA), the peak Australian industry body for the IoT, leading the charge. Its work includes the introduction of an IoT device security certification and the publication of the "Internet of Things security guideline" and "Good data practice: a guide for business to consumer Internet of Things services for Australia", the latter of which aims to assist suppliers of IoT business to consumer (B2C) devices and services to design fair and appropriate privacy and security features to promote take-up, confidence and acceptance by Australian consumers of IoT services and devices.[18] Independent body Standards Australia has also kept Australia in touch with international movements on the IoT in its position on the International Organization for Standardization (ISO) and the International Electrotechnical Commission's (IEC) IoT subcommittee around the development of global standards.

However, the Australian Government has recently announced a 4-year plan to overhaul data regulation, including establishing a National Data Commissioner[19] and new Consumer Data Right (CDR) legislation aimed at providing consumers with open access to and control of their personal data.[20] While the draft legislation has not yet been released, the intent of the CDR appears to mirror the EU's GDPR in many ways. By prioritising data transparency and consumer control, such legislation will necessarily have an impact on businesses manufacturing, supplying and using the IoT.

US

In contrast to Australia, the US has introduced multiple Bills aimed at regulating the IoT, including the Developing Innovation and Growing the Internet of Things (DIGIT) Act S 88 (US) and the Securing the Internet of Things Act of 2017 (US).[21] Much of this legislation has stalled; however, the debate continues about the best path forward. Outside of legislation, the government has also implemented other cybersecurity initiatives. The Federal Communications Commission (FCC) has approved new rules impacting how IoT equipment suppliers conduct their businesses.[22] The Federal Trade Commission (FTC) has also taken enforcement action against IoT providers, including taking D-Link Corporation, one of the largest manufacturers of IoT products, to court.[23] Moreover, the National Institute of Standards and Technology (NIST) has released several reports and recommendations on the IoT, including in relation to cybersecurity standards and a draft IoT-Enabled Smart City Framework around interoperability.[24]

Nevertheless, even in the US there has been some reticence around regulation, with NIST officials making clear statements that such standards are voluntary and insisting the private sector take the lead on adoption.[25]

Europe

With the introduction of the GDPR, Europe has cemented its position as having the strongest data privacy framework worldwide. The GDPR is aimed at protecting the personal data of EU residents, and sets out significant penalties for companies in breach. Europe has also had an independent European Data Protection Supervisor for many years that provides monitoring and advice around protecting personal information and the impact of new technology such as the IoT.[26] Additionally, in November last year, the European Parliament introduced the "objective conformity criteria" aimed at regulating IoT device manufacturing, interoperability and trade.[27]

However, even in Europe there is continued uncertainty about how best to regulate privacy and the IoT. At this year's Computers, Privacy and Data Protection (CPDP) conference, a European Parliament member argued that law enforcement should never have access to certain types of data, and that states should never mandate IoT data retention. Such a stance may lead to conflict with the EU's Police Directive, which governs information collected in a criminal investigation. Some have also criticised the apparent disconnect between Europe's strong privacy laws and the stance of some reports from bodies such as the IoT Security & Privacy Workshop and the European Commission's Digitising European Industry framework, both of which appear to focus more on IoT standardisation and network capacity as challenges to advancing the IoT in Europe.[28]

Asia

If Europe is at the forefront of IoT regulation, then Asia is at the forefront of IoT adoption. A recent Vodafone survey revealed that 36% of Asian companies use IoT devices, with 77% seeing IoT as mission-critical to their business. Interestingly, the survey revealed general optimism about the IoT and security, with 86% of respondents seeing security as an enabler of the IoT and 83% claiming to have adequate skills to manage IoT security.[29]

The IoT is also incredibly important in Asia from a governmental perspective. Singapore and Hong Kong have invested heavily in IoT-connected "smart cities", and many Asian countries are the world's primary IoT device manufacturers. This is reflected in government policy. Singapore has been particularly vocal about the importance of open IoT standards to prevent entrapment by suppliers' "walled gardens", and has published four open IoT standards relating to public area sensor networks, smart homes, interoperability, and IoT reference architecture.[30] In addition, China's Cybersecurity Law, which took effect in June last year, focuses heavily on individual data privacy protection.[31] While the exact scope of the law is yet to be tested, it seems that many businesses that operate IoT infrastructure within China are considered network operators or part of a "critical information infrastructure", subjecting them to additional regulation.[32]

What next

An overview of different global approaches to IoT privacy and security reveals a number of patterns. The first is that there is a general awareness of the IoT's benefits, threats and challenges at every level, from government to enterprise to individual consumers. Secondly, there is a clear tension between consumer distrust in industry self-regulation and government fear of slow-moving laws stifling innovation. Lastly, a strong global consensus is emerging around the importance of adopting open global standards designed to increase both security and interoperability, although how such standards will interact with different regulatory regimes remains to be seen.

In such an environment, there will be no businesses left unaffected by the IoT and its privacy and security challenges. Consequently, every company needs to stay abreast of the developing legal, industry and commercial landscape and take a holistic perspective around their security and privacy strategies. It is no longer enough to simply do your best to comply with applicable regulations and have an up-to-date privacy policy. Businesses will increasingly need to navigate the risk positions, applicable regulatory and quasi-regulatory/industry frameworks, and privacy policies of their partners, suppliers, subcontractors and customers. In short, our clients will need to increasingly take a global perspective on the global opportunities and challenges posed by the IoT.

Albert Yuen
Special Counsel
Gilbert + Tobin
ayuen@gtlaw.com.au
www.gtlaw.com.au

Erica Chan
Lawyer
Gilbert + Tobin
echan@gtlaw.com.au
www.gtlaw.com.au

The authors would like to thank research assistants Kate Dillon, Ashlee Chapman and Natasha Liyanage.

Footnotes

1. L Tung "IoT devices will outnumber the world's population this year for the first time" (7 February 2017) www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/.
2. Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth) (came into effect on 22 February 2018). See also M Fai and L Baranov "Mandatory Data Breach Notification laws are coming … are you ready?" (8 January 2018) www.gtlaw.com.au/insights/mandatory-data-breach-notification-laws-are-coming-are-you-ready.
3. The GDPR represents a complete overhaul of EU data protection law. The GDPR applies across the EU from 25 May 2018, with extraterritorial application. See further information available through the European Commission's GDPR Portal at www.eugdpr.org. See also P Leonard "GDPR: a guide for Australian businesses" (May 2018) www.iot.org.au/wp/wp-content/uploads/2016/12/GDPR-a-guide-for-Australian-businesses.pdf.
4. Office of the Privacy Commissioner of Canada "The Internet of Things: an introduction to privacy issues with a focus on the retail and home environments" (February 2016) www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/iot_201602/.
5. LG CNS "From I.T. to I.O.T.: how the best companies transition to the internet of things" (22 April 2015) www.lgcnsblog.com/features/entrue-world-2015-kevin-ashtons-keynote-speech/#sthash.3nWo00su.dpbs.
6. M Hung "Leading the IoT: Gartner insights on how to lead in a connected world" (2017) www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf.

7. M Heflin "The nervous system of the IoT" (16 August 2016) www.machinedesign.com/iot/nervous-system-iot.
8. A D Rayome "DDoS attacks increased 91% in 2017 thanks to IoT" (20 November 2017) www.techrepublic.com/article/ddos-attacks-increased-91-in-2017-thanks-to-iot/.
9. K Hill and S Mattu "The house that spied on me" (8 February 2018) www.gizmodo.com.au/2018/02/the-house-that-spied-on-me/.
10. *Privacy Commissioner v Telstra Corp Ltd* (2017) 249 FCR 24; 347 ALR 1; [2017] FCAFC 4; BC201700165.
11. ACL, s 3. The definition of "consumer" is extremely broad and is likely to capture a wide variety of IoT devices and services. See also M Swinson, W Osborn and S Swan "There's a glitch in the matrix — the application of consumer guarantees to the IoT" (2017) 21(8&9) *IHC* 176.
12. InfoSec Institute "The top ten IoT vulnerabilities" (February 2018) https://resources.infosecinstitute.com/the-top-ten-iot-vulnerabilities/#gref. See also S Weagle "The rise of IoT botnet threats and DDos attacks" (30 January 2018) www.corero.com/blog/870-the-rise-of-iot-botnet-threats-and-ddos-attacks.html and N Fearn "What the Internet of Things (IoT) means for data security" (28 March 2018) www.itpro.co.uk/internet-of-things-iot/30844/what-the-internet-of-things-iot-means-for-data-security.
13. This view was raised in R Bosua "Privacy by design in the era of the Internet of Things (IoT)" (2016) 3(1-2) *MTC* 3.
14. Gartner "Gartner says worldwide IoT security spending will reach $1.5 billion in 2018" (21 March 2018) www.gartner.com/newsroom/id/3869181.
15. The Economist Intelligence Unit *What the Internet of Things Means for Consumer Privacy* (2018) https://perspectives.eiu.com.
16. As IoT solutions communicate over a telecommunications or radio network, a service provider of the IoT connectivity may be regulated by applicable Australian telecommunications or radio communications laws such as the Telecommunications Act 1997 (Cth) or the Radiocommunications Act 1992 (Cth). Many IoT devices are low-powered devices that are permitted to operate in designated spectrums under the Radiocommunications (Low Potential Interference Devices) Class Licence 2015 (Cth). Mobile phone users are permitted to use their mobile phones and devices that use SIM cards by the Radiocommunications (Cellular Mobile Telecommunications Devices) Class Licence 2014 (Cth). Subject to exemptions, where the IoT device passing over a telecommunications system has communications interception capabilities, the Telecommunications (Interception and Access) Act 1979 (Cth) may also need to be considered.
17. OAIC "Guide to data analytics and the Australian Privacy Principles" (March 2018) www.oaic.gov.au/resources/agencies-and-organisations/guides/guide-to-data-analytics-and-the-australian-privacy-principles.pdf.
18. IoTAA "Strategic plan to strengthen IoT security in Australia" (September 2017) www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Strategic-Plan-to-Strengthen-IoT-Security-in-Australia-v4.pdf; IoTAA "Internet of Things security guideline" (November 2017) www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf; IoTAA "Good data practice: a guide for business to consumer Internet of Things services for Australia" (November 2017) www.iot.org.au/wp/wp-content/uploads/2016/12/Good-Data-Practice-A-Guide-for-B2C-IoT-Services-for-Australia-Nov-2017.pdf. See also A Yuen "Seizing the IoT opportunity: IoTAA good data practice guide for B2C IoT services" (10 November 2017) www.gtlaw.com.au/insights/seizing-iot-opportunity-iotaa-good-data-practice-guide-b2c-iot-services.
19. P Bhunia "Australian Government announces A$65 million investment to reform country's data system" (2 May 2018) www.opengovasia.com/articles/australian-government-announces-a-65-million-investment-to-reform-countrys-data-system.
20. S Venkat "Australia mulls over new Consumer Data Right legislation" (29 November 2017) www.cerillion.com/Blog/November-2017/Australia-new-Consumer-Data-Right-legislation.
21. K Goodloe "Covington IoT update: U.S. legislative roundup on IoT" (9 May 2018) www.natlawreview.com/article/covington-iot-update-us-legislative-roundup-iot.
22. R Quirk "High-level overview of the FCC's equipment regulation changes — IoT device suppliers beware" (21 July 2017) www.iotforall.com/overview-fcc-equipment-regulation-changes/.
23. K C Halm and A Reynolds "IoT vendors beware: FTC's latest enforcement action signals further scrutiny of the industry" (23 January 2017) www.privsecblog.com/2017/01/articles/dataprotection/iot-vendors-beware-ftcs-latest-enforcement-action-signals-further-scrutiny-of-the-industry/.
24. NIST "What is the Internet of Things (IoT) and how can we secure it?" www.nist.gov/topics/internet-things-iot.
25. D B Johnson "Why is no one raising a hand to regulate the internet of things?" (16 March 2018) https://fcw.com/articles/2018/03/16/iot-regulation-ispab-johnson.aspx.
26. European Data Protection Supervisor "Internet of Things" https://edps.europa.eu/data-protection/our-work/subjects/internet-things_en.
27. D Meyer "European Parliament pushes on IoT device security and interoperability" (4 December 2017) https://internetofbusiness.com/iot-devices-get-new-security-interoperability-obligations-eu/.
28. L Krahulcova "What the EU is getting wrong about the Internet of Things" (12 February 2018) www.accessnow.org/what-the-eu-is-getting-wrong-about-the-internet-of-things/.
29. A Tan "Asia is pace-setter in IoT" (23 November 2017) www.computerweekly.com/blog/Eyes-on-APAC/Asia-is-pace-setter-in-IoT.
30. A Tan "Singapore government outlines its approach to IoT" (21 March 2018) www.computerweekly.com/news/252437239/Singapore-government-outlines-its-approach-to-IoT. See also,

Information Technology Standards Committee "Internet of Things Technical Committee (IOTTC)" www.imda.gov.sg/itsc/technical-committees/internet-of-things-technical-committee-iottc.

31. IT Advisory KPMG China "Overview of China's Cybersecurity Law" (February 2017) https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf.

32. M Parsons "IoT cybersecurity and data privacy trends in Asia: be ready" (13 June 2017) www.lexology.com/library/detail.aspx?g=78e15982-230e-4990-a635-f348fd688b8e.

Privacy Law
Bulletin

Watch out for spit parties: privacy questions about recreational genomics

Dr Bruce Baer Arnold *UNIVERSITY OF CANBERRA*

Abstract

This article looks at the privacy aspects of recreational genomics, an emerging industry in which consumers gift or sell genomic data to find an association with ancestors or identify supposed susceptibility to genetic disorders. Salient privacy concerns include gifting of data that encompasses biological relatives and the use by law enforcement agencies of large-scale private sector genomic databases.

Introduction

May 2018 saw practitioner and media coverage of the Australian Health Department's belated announcement regarding arrangements for people to opt out of aspects of the national My Health Record (MyHR) medical data scheme. Outside of the tabloids, there was less coverage of an incident in the US involving what has been variously dubbed recreational genomics or direct-to-consumer genetic testing. In that incident, law enforcement personnel accessed a large-scale private sector genomic database in order to target the identity of a serial killer. This article offers an introduction to recreational genomics and highlights privacy issues for Australian legal practitioners and consumers.

Salient points for practitioners are:

- After a somewhat rocky childhood, the recreational genomics sector is maturing and we will see increasing participation by Australian consumers.
- The leading services are located overseas and there are questions about the effectiveness of privacy protections for Australian consumers.
- The particular characteristics of genomic data mean that data collection, processing and storage pose challenges that may be qualitatively different to that of credit card and other financial data.

The genomics genie

Over the past 50 years, researchers and clinicians have increasingly been able to read what some scientists dub "the book of life", ie the genetic code found in all humans and other animals.[1] That code can be identified using tools that are increasingly becoming more reliable, faster and cheaper, particularly where a factory-style system deals with data from very large numbers of people. The code can be expressed in ways that are readily sorted by computers and associated with demographic or other data such as age, gender, lineage and medical history. The expectation is that a large-scale database — covering millions of people or even a whole population — will provide useful information. Such information might for example provide the basis for the personalised medicine, including individual-specific pharmaceuticals, that is attracting major public/private sector funding overseas. Gaining useful information is a challenging task, because although we can identify the genomic code — put simply, we can read the letters — we cannot comprehensively understand what the words formed by those letters always mean. Researchers, unlike some policy advocates and journalists, will accordingly often caution that correlation is different to causation, that lifestyle (or exposure to particular harms such as nicotine) may be as significant as a particular gene or set of genes, and that care should be taken in interpreting genomic data. Put simply, we read but do not necessarily understand the book of life; DNA is not necessarily destiny.[2]

There has been understandable excitement about the potential of genomic research, consistent with the faith in science fostered by achievements over the past century. That excitement, alongside ongoing reductions in the cost of genomic data processing and the perceived benefits for investors in the emerging biotech economy, has fostered the emergence of recreational genomics.[3] Organisations in that sector operate globally on a commercial or not-for-profit basis, targeting consumers in advanced economies such as Australia (unlike past bioprospecting initiatives such as the controversial "vampire project" that gathered samples from indigenous people in the Third World).[4] Their operation raises questions about the capacity of health and other regulators across and within jurisdictions. Saliently, it raised questions about consumer understanding and recourse if there is a disregard of privacy.

Spit, ancestors and ailments

Devices for identifying genomic code are expensive and high-tech, although becoming cheaper and thus found in a range of locations apart from criminal forensics laboratories and leading research institutions. Recreational genomics is founded on the simplicity of data collection and omits any referral by or consultation with a consumer's general practitioner.

It does not require a consumer to visit a laboratory in person, experience the pain many people associate with giving a blood sample or even visit a health practitioner. Instead all that is required is that each consumer painlessly and conveniently uses a swab to scrape a few cells from inside their mouth, with that buccal swab being placed in a test tube sized container that is mailed to the genomic service provider along with payment. The sample, once received by that provider, is processed as a genetic code and added to a database that contains the code from other contributors, typically people located across the globe. The contributor of the sample receives a report online or in hard copy. Typically that consumer also has access to raw data that can be downloaded for provision to another entity or shared through an "open DNA" site such as GEDMatch.

Some service providers such as AncestryDNA[5] and Family Tree DNA are associated with genealogical businesses or not-for-profits, promoting their "family finder" or "relative finder" services as a way of establishing affinity with biological relatives over many generations and making links with figures such as Elvis Presley, Bill Clinton or Queen Elizabeth.[6] Such "ancestral" services are gathering data from large numbers of participants, both because it can be entertaining to know that you are a distant relative of people who are famous or infamous and because there is a sense that research associated with bodies such as the US National Geographic Society will advance knowledge.[7] Other services are associated with insurers. In 2010 for example, Australian insurer NIB faced criticism for offering its customers access to discounted genomic profiling services provided by US-based Navigenics.

Recent years have seen the emergence of more overtly commercial services. Two of the most prominent are 23andMe (drawing on participants in Australia, Europe and North America)[8] and deCODE (which sought to map the genes of everyone in Iceland).[9] There have been services operating out of Bulgaria, Singapore, India and other locations. We will presumably see services operating out of China, given the emphasis placed by the government of the People's Republic of China on investment in biotech.[10]

US-based 23andMe gained publicity for so-called spit parties — publicity events at which celebrities drank wine, ate canapés, mingled with other glitterati and provided their buccal swabs to the organisers. The company has encountered difficulties with US regulators (discussed below) but has attracted participants from across Australia and is likely to do so in future. It is perhaps the most prominent example of recreational genomics, building a large database with a global spread and providing reports directly to the consumers without mediation by a general practitioner, other clinician or medical institution. Those reports may be misinterpreted by some readers, at worst resulting in self-harm by consumers who misunderstand risk and believe that DNA is destiny.

There is disagreement about the business model/s underlying overtly commercial recreational genomics. With sufficient scale, there appears to be scope for business to be profitable merely by processing samples, converting them to data and providing consumers with a report that offers broad information about affinities and offers some analysis about genomic attributes, for example correlations between specific genes and the claimed likelihood of particular ailments. We can think of that reporting as a grandchild of traditional actuarial tables with which insurers have identified risk and forecasted probable lifespans on the basis of an individual's consumption of tobacco and alcohol, and occupation. As with such tables, the bigger the database, the more the prediction is likely to be accurate, and consumers might alter their behaviour and thus mitigate risk on receiving a report.

There has however been speculation that the genomics corporations are ultimately less interested in providing reports to consumers across the globe and are instead seeking to build a very detailed and large-scale repository of genomic data that could be mined by pharmaceutical businesses and other entities. The value lies in the scope and scale of the data that is collected rather than in making money by entertaining consumers at around $99 per head. It is unclear whether most consumers have much sense of what might be done with data from buccal swabs they have provided, whether there are any risks regarding data security (despite publicity in the US about data breaches involving clinics and health service organisations), and whether they have remedies under contract or consumer protection law.[11]

From a regulatory perspective, we can differentiate recreational genomics from data collection and provision associated with leading research institutions. Australia's world-class Garvan Institute of Medical Research has for example invited people to "explore your genome" and in May 2018 launched a GoExplore initiative in which the fee ($4400) is more than 20 times that of the recreational sector, referral by a general practitioner is

required, data is handled within Australia, expert advice is provided by specialists, and practice is bounded by Australian clinician/research codes.

Genomic big data

Law enforcement agencies embraced DNA technologies well in advance of the emergence of the direct-to-consumer genomic testing sector. Forensic genomic databases have been so normalised as to be taken for granted. Most legal practitioners are familiar with the existence of criminal forensic databases, whether through discussion during their legal education (for example as part of crime and evidence law units) or along with the population at large as part of depictions in popular culture such as the *CSI* television series or novels in which a telltale drop of blood identifies the rapist, murderer or burglar.[12]

Perhaps unsurprisingly, there have been calls for mandatory or voluntary provision of DNA on a population scale to quickly identify criminals, reduce identity crime or even allow the speedy identification of victims after a terrorist incident. Those calls are an echo of proposals for whole of population fingerprinting that were criticised as disproportionate and potentially misused. In Australia, we are accustomed to DNA collection from criminal suspects, with collection and data matching founded on statute law and akin to the provision/matching of fingerprints. There has not been support in Australia for mandatory data collection such as that announced in the Middle East in recent years. Dubai for example indicated in February 2018 that all residents (starting with nationals) would be profiled for health purposes, albeit there is some uncertainty about access by intelligence services. A Kuwait counterterrorism statute in 2015, following a terrorist bombing, required data collection from 2.9 million foreign residents and 1.3 million citizens alike, with imprisonment as a sanction for noncompliance.

Proponents of such schemes typically argue that they are imperative for national security or law enforcement, that people who have nothing to hide have nothing to fear, and that — akin to the construction of population-scale facial biometric databases through for example passport and driver registration schemes — they are benign because provision of a buccal swab is less invasive than providing a blood sample. A response from critics is that mass collection is disproportionate, is not necessarily effective and poses risks regarding data security. It is axiomatic, for example, that a person can change their identity number, name, credit card/bank number, citizenship or even gender but cannot change their genome. It is potentially an immutable identifier, an indelible genetic fingerprint.

Matching a murderer

Where does recreational genomics come in? Earlier this year, US police identified alleged rapist and serial killer Joseph DeAngelo by conducting searches on the GEDmatch genomic open data site.[13]

That site has hitherto attracted little scholarly attention from the legal and law enforcement communities, instead being known among genealogists. GEDmatch is not a government database and is not operated by a research institution. It accepts genomic data from people who have tested with AncestryDNA, Family Tree DNA and 23andMe. Those people assume responsibility for uploading data about themselves for sharing with others who have an interest in social connection, ie building family trees by matching data that identifies people who are known to be biological relatives and those who are not known.

The police used GEDmatch without a need for a warrant under state or federal law. It appears that any entity could do so. The searches enabled them to identify DeAngelo with sufficient certainty to persuade the court to order a test that appears to have directly matched archived crime scene samples. In essence, using a genomic open data tool offered a mechanism for solving a cold case.

On that basis we can expect to see media coverage and litigation in the US about access to genomic open data resources and to proprietary genomic databases maintained by corporations such as 23andMe. We can also expect to see controversy in Australia about court-authorised access to Australian genomic databases.

Fuzzy privacy, weak consumer protection?

From a privacy perspective, the salience of recreational genomics lies in biological relationships. There is some commonality between biological relatives; your genetic profile for example has much of the same genomic data as that of your biological parents, siblings and offspring. You might accordingly be identified with varying degrees of precision using data that relates to those relatives. That identification might allow inferences about your appearance or your susceptibility to particular disorders, irrespective of whether those disorders have become manifest and irrespective of whether you wish to privately acknowledge or publicly disclose them.

Research over the past decade has accordingly highlighted a range of questions for legal practitioners, ethicists and policymakers. One question is the accuracy of the testing,[14] with for example claims that the quality of processing in some Eastern European facilities is egregiously low and that some services verge on being fraudulent. There has not been significant action by

consumer protection agencies at the national level or by disgruntled customers, perhaps because there wasn't major reliance on the tests or because consumers were unaware that consumer law offered a meaningful remedy.

It is important to recognise that dominant service providers offer different tests and may well provide a specific consumer with somewhat different results. Regulators have expressed concern about what might be considered to be diagnostic services outside a conventional regulatory framework that encompass registration and supervision of health service providers alongside certification of clinicians and adherence to formal research codes. There is no global Genomic Data Right, unsurprising given the late establishment of the finance/utilities sector of the Consumer Data Right announced in Australia in May 2018. There is disagreement about genetic discrimination frameworks.[15] Calls for a global Genomic Privacy Convention (akin to the European General Data Protection Regulation discussed in recent issues of this bulletin) have gained little traction and are often opposed as contrary to the achievement of social goods through advancement of health research.[16]

A convention is of interest because the Australian Constitution is silent about privacy and makes no mention of the genome. The Commonwealth under its external affairs, posts and customs heads of power has scope to shape consumption of recreational genomic services. Its emphasis for the moment appears to be investment in genomics research (notably the $500 million Australian Genomics Health Futures Mission announced in May this year, similar to larger initiatives in the UK and the US) and public education campaigns.[17] The effectiveness of education is uncertain, given the respect we owe to life science researchers and the willingness of leading geneticists to share their genomic samples.[18]

Education is significant because unconsidered sharing of genomic data is not caring but is not actionable. Put simply, there is no restriction on a relative gifting or selling a sample — a skin scraping, blood or saliva — from their own body to a genomic service provider. It is their property, not yours, even though it might offer a view of you, potentially a view contrary to your values about disclosure.[19] It can be converted into data that is an asset of a corporation and over which neither the consumer nor you have much control outside the typically expansive terms and conditions used by the service provider to limit corporate liability and assert corporate rights.

Such unilateral sharing without your authorisation and indeed without your knowledge, given that there is no requirement to alert you that a biological relative has participated in a recreational genomic program, is potentially significant because recreational genomic services are currently based overseas. Australian consumers are perforce reliant on an understanding of contractual provisions regarding the sale/gifting of samples (ineffective if your client was not the individual providing that sample), trust that the service will meet contractual obligations and remain in a position to meet obligations (are all bets off if the service is liquidated or its trove of data is acquired?), and hope that overseas regulators such as the US Food and Drug Administration or Federal Trade Commission have both the power and interest in policing inadequate practice. The increasing body of knowledge about the feasibility of re-identification of what was claimed to be adequately anonymised health data should pose cautions,[20] as should controversy over initiatives such as the UK care.data program.[21]

Locally it's unclear whether the Office of the Australian Information Commissioner has the technical skills and the willingness to look beyond traditional stakeholders, in essence its regulatory capture by medical researchers that is sufficient to offset indifference on the part of the Therapeutic Goods Administration and the imperatives that drive the National Health and Medical Research Council.[22]

There is value in the emergence of an Australian direct-to-consumer genomic service sector, one that is globally competitive on the basis that it both embodies technical best practice (in contrast for example to past services in the former Soviet bloc) and recognises concerns regarding genomic privacy. There is no simple solution that will effectively address tensions regarding access to bulk/individual data, meaningful consent by those people who sell/gift samples, and respect for the dignity in terms of autonomy of those people who will be tacitly mapped through the action of their relatives. It is difficult for example to conceptualise a right to genomic obscurity outside action by governments to require both de-identification of genomic data about yourself and family members and enforcement of stronger standards to significantly inhibit data breach.

A starting point for engagement by leading law firms with such questions and shaping of practice frameworks for the coming biotech century is a recognition that genomic data is special: the book of life is more valuable and less tractable than the book of telephone numbers or the electronic folders of bank account details that were apparently misplaced by the Commonwealth Bank 2 years ago.

Dr Bruce Baer Arnold
Associate Professor
University of Canberra
www.canberra.edu.au

About the author
Associate Professor Bruce Baer Arnold teaches privacy, confidentiality, health and consumer law at the University of Canberra.

Footnotes

1. E Pennisi "Finally, the book of life and instructions for navigating it" (2000) 288(5475) *Science* 2304.
2. W Bonython and B B Arnold "Privacy, personhood, and property in the age of genomics" (2015) 4(3) *Laws* 377.
3. K Davies, *The $1,000 Genome: The Revolution in DNA Sequencing and the New Era of Personalized Medicine*, Simon & Schuster, 2010; P Su "Direct-to-consumer genetic testing: a comprehensive view" (2013) 86(3) *The Yale Journal of Biology and Medicine* 359.
4. M Dodson and R Williamson "Indigenous peoples and the morality of the Human Genome Diversity Project" (1999) 25(2) *Journal of Medical Ethics* 204.
5. Available at www.ancestry.com/dna/.
6. J K Wagner, J D Cooper, R Sterling and C D Royal "Tilting at windmills no longer: a data-driven discussion of DTC DNA ancestry tests" (2012) 14(6) *Genetics in Medicine* 586; U A Perego, A Turner, J E Ekins and S R Woodward "The science of molecular genealogy" (2005) 93 *National Genealogical Society Quarterly* 245.
7. S Wells, *Deep Ancestry: Inside the Genographic Project*, 1st edn, National Geographic, 2006.
8. Available at www.23andme.com.
9. M Fortun, *Promising Genomics: Iceland and deCODE Genetics in a World of Speculation*, University of California Press, Berkeley, 2008; D Winickoff, "A Bold Experiment: Iceland's Genomic Venture" in *Ethics, Law and Governance of Biobanking*, D Mascalzoni (Ed), Springer Netherlands, 2015, p 187.
10. K Birch "The neoliberal underpinnings of the bioeconomy: the ideological discourses and practices of economic competitiveness" (2006) 2(3) *Genomics, Society, and Policy* 1; R Benjamin "A lab of their own: genomic sovereignty as postcolonial science policy" (2009) 28 *Policy and Society* 341.
11. C S Kruse, B Frederick, T Jacobson and D K Monticone "Cybersecurity in healthcare: a systematic review of modern threats and trends" (2017) 25(1) *Technology and Health Care* 1.
12. S Krimsky and T Simoncelli, *Genetic Justice: DNA Data Banks, Criminal Investigations, and Civil Liberties*, Columbia University Press, New York, 2012; D Lazer (Ed), *DNA and the Criminal Justice System: The Technology of Justice*, MIT Press, 2004.
13. A Regalado "Investigators searched a million people's DNA to find Golden State serial killer" (27 April 2018) www.technologyreview.com/s/611038/investigators-searched-a-million-peoples-dna-to-find-golden-state-serial-killer/.
14. R Kalf, R Bakker and C Janssens "Predictive ability of direct-to-consumer pharmacogenetic testing: when is lack of evidence really lack of evidence?" (2013) 14(4) *Pharmacogenomics* 341; M Murray "Why we should care about what you get for 'only $99' from a personal genomic service" (2014) 160(7) *Annals of Internal Medicine* 507.
15. G van Ommen and M Cornel "Recreational genomics? Dreams and fears on genetic susceptibility screening" (2008) 16 *European Journal of Human Genetics* 403; J H Gerards, A W Heringa and H L Janssen, *Genetic Discrimination and Genetic Privacy in a Comparative Perspective*, 1st edn, Intersentia, 2005.
16. S Harmon "The significance of UNESCO's Universal Declaration on the Human Genome and Human Rights" (2005) 2(1) *SCRIPTed* 18.
17. B Potter "Federal Budget 2018: Bill Ferris gets his human genome 'moonshot'"*Australian Financial Review* 9 May 2018 www.afr.com/news/policy/budget/federal-budget-2018-bill-ferris-gets-his-human-genome-moonshot-20180509-h0zuc6.
18. A Harvey "Genetic risks and healthy choices: creating citizen-consumers of genetic services through empowerment and facilitation" (2010) 32(3) *Sociology of Health & Illness* 365; D E Winickoff and L B Neumann "Towards a social contract for genomics: property and the public in the 'Biotrust' model" (2005) 1(3) *Genomics, Society, and Policy* 8.
19. W Bonython and B B Arnold "Direct to consumer genetic testing and the libertarian right to test" (2017) *Journal of Medical Ethics*; R A Spinello "Property rights in genetic information" (2004) 6(1) *Ethics and Information Technology* 29; A George "The difficulty of defining 'property'" (2005) 25(4) *Oxford Journal of Legal Studies* 793.
20. K El Emam, E Jonker, L Arbuckle and B Malin "A systematic review of re-identification attacks on health data" (2011) 6(12) *PloS ONE* e28071; K El Emam, *Guide to the De-Identification of Personal Health Information*, CRC Press, 2013.
21. J Keen, R Calinescu, R Paige and J Rooksby "Big data + politics = open data: the case of health care data in England" (2013) 5(2) *Policy & Internet* 228; P Carter, G T Laurie and M Dixon-Woods "The social licence for research: why care.data ran into trouble" (2015) 41 *Journal of Medical Ethics* 404; J Hoeksma "The NHS's care.data scheme: what are the risks to privacy?" (2014) 348 *British Medical Journal* g1547; P Vezyridis and S Timmons "Understanding the care.data conundrum: new information flows for economic growth" (2017) 4(1) *Big Data & Society* 1.
22. B B Arnold and W Bonython "Sharing the book of life: privacy, the new genomics and health sector managers" (2015) 12(4) *Privacy Law Bulletin* 103; B B Arnold and W Bonython "Australian reforms enabling disclosure of genetic information to genetic relatives by health practitioners" (2014) 21(4) *Journal of Law and Medicine* 810; J Siganto and M Burdon "The Privacy Commissioner and own-motion investigations into serious data breaches: a case of going through the motions?" (2015) 38(3) *University of New South Wales Law Journal* 1145.

Is the repeal of US privacy regulations a victory for digital advertising?

Richard Newman *HINCH NEWMAN LLP*

Privacy and data security-related issues have received a significant amount of attention recently, particularly as it pertains to the Federal Trade Commission's (FTC) enforcement of unfair or deceptive practices involving the collection and use of consumers' information. Juxtaposed with US regulators' continued efforts to aggressively pursue privacy violations across a wide range of industries, including those that involve children and the Internet of Things, is the new administration's lessening of restraints on sharing personal information.

Against this backdrop, Obama-era privacy rules passed in 2016 by the Federal Communications Commission (FCC), which were intended to provide internet users with greater control over how service providers could use personal data, were repealed in April 2017. The 2016 rules required, amongst other things, that internet service providers (ISPs) have express permission from their customers prior to sharing certain personal information with third-parties, including third-party marketers. Such personal information includes, without limitation, location data, browsing history, app usage, geolocation data, financial data and health information.

Not surprisingly, the resolution has received an enormous amount of backlash from Democrats, civil liberties groups and other advocates of online rights. It has also received support from telecommunications companies that believe the repealed privacy regulations — that never went into effect — would have unfairly restricted broadband providers' ability to compete with tech companies that serve targeted advertisements without the same privacy framework.

The regulations were repealed pursuant to the Congressional Review Act (US) (CRA), a tool that permits Congress to repeal regulations if a joint resolution is passed by both the House and Senate, and signed by the President. Simply stated, the CRA provides Congress with the ability to revoke recently enacted regulations adopted under the prior administration. The significance of the CRA does not lie solely in the mechanism it provides to repeal federal regulations. Rather, the CRA also prohibits federal agencies from enacting substantially similar regulations in the future.

FCC Chairman Ajit Pai has stated that he believes the privacy rules passed in the final days of the Obama administration were designed to benefit one group of favoured companies, not online consumers. He has also stated that the FTC, not the FCC, should police such data use.

Consequently, the repeal has shifted regulatory power back to the FTC. The FCC and FTC have also recently announced the intent to enforce uniform privacy rules consistent with FTC guidance, including those pertaining to transparency and the implementation of reasonable data security measures. The agreement to coordinate online consumer protection efforts and enforcement responsibilities outlines the process by which the FCC and FTC will seek to safeguard the public interest.

As stated by Chairman Pai: "Instead of saddling the Internet with heavy-handed regulations, we will work together to take targeted action against bad actors." The FTC has also made clear its commitment to "ensuring that Internet service providers live up to the promises they make to consumers".[1]

It is anticipated that the FCC and FTC will work together to protect consumers by, without limitation, reviewing informal complaints concerning ISPs, including the accuracy of disclosures that they provide to consumers and other unfair practices involving network management practices, performance and commercial terms of service.

ISPs remain subject to statutory privacy provisions, including state laws that govern privacy and breach notification. However, privacy and consumer advocates believe that broadband providers are now licensed to collect browsing histories and other personal data and sell them to third parties for marketing purposes with very little regulatory oversight or fear of enforcement.

Privacy advocates also criticise the regulatory paradigm shift on the basis that major ISPs' informal pledges not to sell customers' individual internet browsing information are merely voluntary, at best; that there are no assurances that ISPs will decide to implement contractual privacy protection. Criticism is also based upon the FTC's broad enforcement, not rule-making authority.

The prevailing view is that the resolution is a significant victory for the digital advertising and telecom industries, as well as tech innovators. ISPs such as AT&T Inc, Comcast Corporation and Verizon Communications Inc are believed to possess voluminous data about users, including anonymised profiles, and are able to provide highly customised advertisements. However, it is too soon to know just how valuable data collection may be for ISPs.

Ironically, repeal of rules that would have provided US consumers with greater control over the use of their data coincides with the implementation of regulations governing the use of personal data belonging to citizens of the European Union, effective as of 25 May 2018. The General Data Protection Regulation is specifically designed to protect the privacy of European Union citizens by giving them the ability to dictate how their information is collected, processed, managed and stored. The foregoing rights include, without limitation, the right to explicitly consent to how their personal data is utilised and the right to have such use discontinued.

Simultaneously, in an effort to encourage free marketing competition, the FCC has reversed the Obama-era net neutrality rules enacted in 2015. The "Restoring Internet Freedom Order" reclassifies broadband internet as an "information service", thereby subjecting it to lightened regulation outside of the FCC's authority.

Restrictions that previously barred ISPs from blocking, throttling or prioritising data speed have been lifted. The order also requires ISPs to publicly disclose accurate information regarding network management practices, performance characteristics and commercial terms of its broadband services sufficient to enable consumers to make informed choices regarding the purchase and use of such services and entrepreneurs and other small businesses to develop, market and maintain online offerings. The disclosure must be made via a publicly available and easily accessible website or through transmittal to the FCC.

The repeal is yet to take effect. The order must first be approved by the Office of Management and Budget following an assessment of ISP web traffic disclosure obligations. The FCC will then publish another notice in the Federal Register announcing the effective date.

Many believe that the delay is a stalling tactic designed to place more pressure on Congress to pass a new net neutrality law.

Net neutrality proponents believe that ISPs should be freely permitted to control how information is accessed. Conversely, critics such as many in the digital marketing industry believe that granting ISPs the ability to prioritise content speed will tilt the playing field in favour of tech giants and harm the ability of small businesses to compete in the global marketplace.

FCC Commissioner Jessica Rosenworcel, a Democrat who voted against repeal, stated:

> This is profoundly disappointing.
> The agency failed to listen to the American public and gave short shrift to their deeply held belief that Internet openness should remain the law of the land. The agency turned a blind eye to serious problems in its process — from Russian intervention to fake comments to stolen identities in its files.[2]

The Restoring Internet Freedom Order pre-empts states from adopting more stringent ISP-specific legislation or regulations. In March, however, Washington became the first state to pass legislation prohibiting ISPs from prioritising different types of website traffic. Governors of Montana, New Jersey, New York and Vermont have also signed net neutrality executive orders.

Additionally, a California Bill that seeks to impose strict net neutrality requirements was recently approved by a Senate Judiciary Committee. It seeks to ban throttling and paid data-cap exemptions. The Bill requires approval from the Senate Committee on Appropriations, the state Senate and Governor Jerry Brown.

A coalition of state attorneys-general has also initiated legal action against the FCC. Broadband lobbying groups have publicly stated an intention to file lawsuits if states impose net neutrality rules, arguing that the FCC possesses authority to pre-empt local laws.

These materials are provided for informational purposes only and are not to be considered legal advice, nor do they create a lawyer–client relationship. No person should act or rely on any information in this article without seeking the advice of an attorney. Information on previous case results does not guarantee a similar future result.

Richard Newman
Managing Partner
Hinch Newman LLP
rnewman@hinchnewman.com
www.hinchnewman.com
https://ftcdefenselawyer.com

About the author

Richard Newman is an internet marketing compliance and regulatory defense attorney at Hinch Newman LLP focusing on advertising and digital media matters. His practice includes conducting legal compliance reviews of advertising campaigns, representing clients in investigations and enforcement actions brought by the Federal Trade Commission and state attorneys-general, commercial litigation, advising clients on promotional marketing programs, and negotiating and drafting legal agreements.

Footnotes

1. FCC "FTC, FCC Outline Agreement to Coordinate Online Consumer Protection Efforts Following Adoption of the Restoring Internet Freedom Order: Federal Agencies Intend to Sign Memorandum of Understanding to Allocate Enforcement Responsibilities" (11 December 2017) https://apps.fcc.gov/edocs_public/attachmatch/DOC-348191A1.pdf.
2. FCC "Statement of Commissioner Jessica Rosenworcel on Tomorrow's Federal Register Publication of the End of Net Neutrality" (10 May 2018) https://apps.fcc.gov/edocs_public/attachmatch/DOC-350644A1.pdf.

For editorial enquiries and unsolicited article proposals please contact Aidan Fisher at aidan.fisher@LexisNexis.com.au or (02) 9422 8908
Cite this issue as (2018) 15(5) *Priv LB*
SUBSCRIPTION INCLUDES: 10 issues per volume plus binder www.lexisnexis.com.au
SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067
CUSTOMER RELATIONS: 1800 772 772
GENERAL ENQUIRIES: (02) 9422 2222
ISSN 1449-8227 Print Post Approved PP 243459/00067 This newsletter is intended to keep readers abreast of current developments in the field of privacy law. It is not, however, to be used or relied upon as a substitute for professional advice. Before acting on any matter in the area, readers should discuss matters with their own professional advisers.