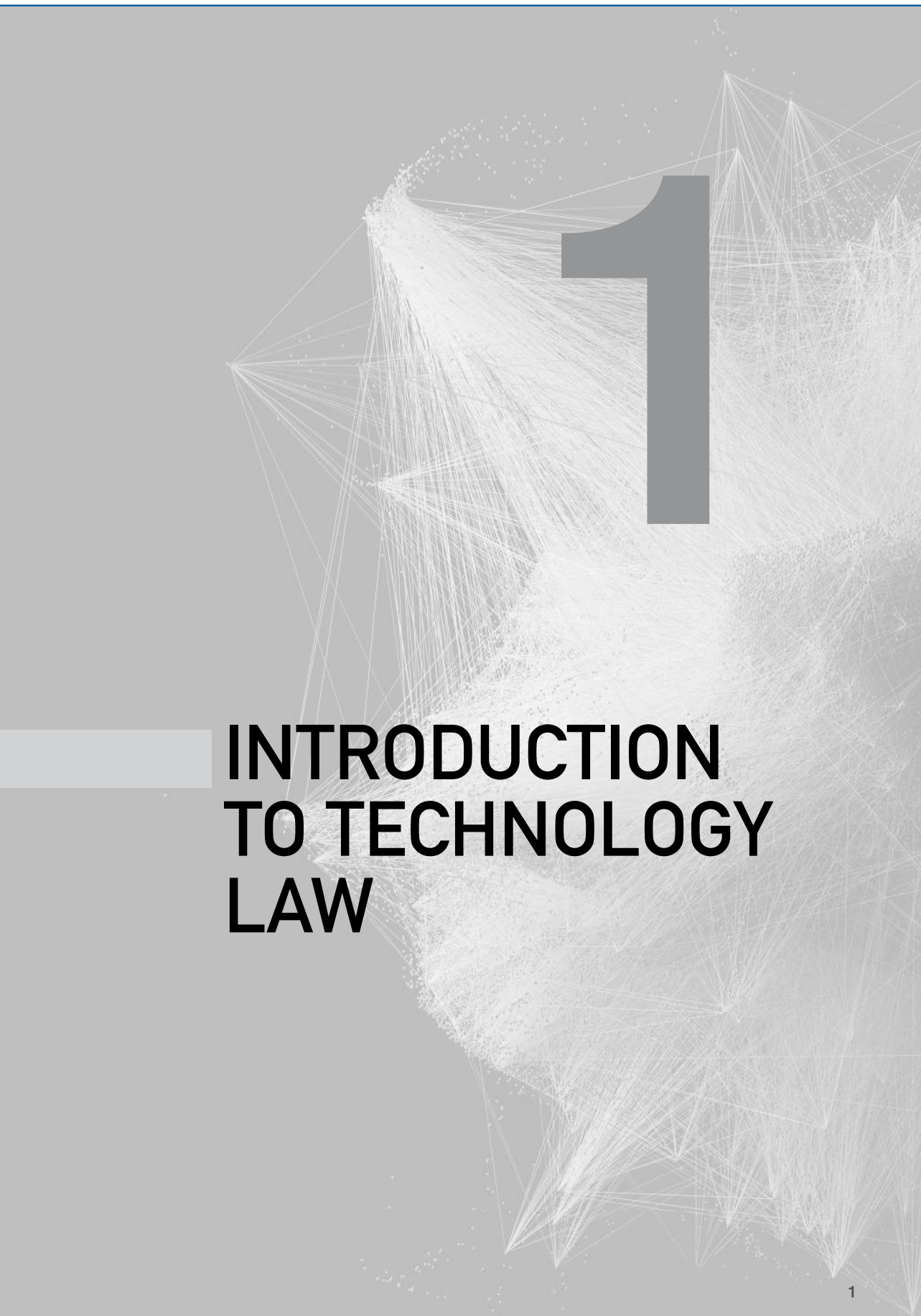

1

INTRODUCTION TO TECHNOLOGY LAW

Conceptualising technology law

In recent decades, the regulation of technology and associated information has become an important and topical area of law, relevant to almost all aspects of society. Issues in technology law typically extend beyond specific jurisdictions and have state, national and international implications. Developments in one jurisdiction rapidly have international ramifications, due to the connectedness facilitated by the internet and modern communications technology. The areas of the law that are evolving due to technological developments are diverse: a preliminary list would include finance law, criminal law, medical law, media law and privacy law. New technology creates challenges, because when it becomes available, new regulatory gaps arise. For example, the emergence of cryptocurrencies such as Bitcoin has required public agencies to issue guidelines as to whether they constitute forms of currency, and whether dealings using them are subject to taxation laws.[1] Another example is the legislation enacted in the early 2000s to regulate the use of DNA evidence in criminal investigations. When these laws were enacted, the use of commercial ancestry databases and other modern techniques in genetic analysis to identify suspects in some high-profile contemporary cases was not envisaged.[2]

A primary consideration must be the concept and definition of technology law. As a relatively new area of the law, there has been debate over the definition and coherence of technology law as a field of legal expertise and scholarship. As a somewhat nebulous field, it is similar in this respect to other more recent and diverse fields of the law, such as health or environmental law. Technology law combines several traditional areas of the law and appears to borrow from other fields, such as criminal law, human rights law, privacy law, and political and regulatory theory.[3] One issue for technology law is that there is such a wide range of different technologies, each being applied in various contexts. These all have risks and benefits that must be managed to prevent harms from occurring. Further, adequate regulation in the form of legislation, judicial oversight, policies, standards and procedures spread across different areas of the legal system, fields of business, government agencies, and state, national and international jurisdictions equates to a major challenge for regulators attempting to adopt effective and coherent approaches.[4]

There have been numerous attempts to define the field of technology law. Until the mid-2000s, it was disjointed, lacking a cohesive theory. As more prominent legal issues arose that did not fit well within the existing paradigms, it became recognised that a new field of law was needed to determine 'how to protect interests in particular cases as well as how a decision will affect other interests once it is integrated within the whole law'.[5] From

1 Parliament of Australia, Senate Economics References Committee, *Digital Currency – Game Changer or Bit Player* (August 2015). Available: <www.aph.gov.au/parliamentary_business/committees/senate/economics/digital_currency/~/media/Committees/economics_ctte/Digital_currency/report.pdf>. See, also, Australian Taxation Office, *Tax Treatment of Crypto-Currencies in Australia – Specifically Bitcoin*. Available: <www.ato.gov.au/general/gen/tax-treatment-of-crypto-currencies-in-australia---specifically-bitcoin> (last updated 18 June 2019).

2 Chris Phillips, 'The Golden State Killer Investigation and the Nascent Field of Forensic Genealogy' (2018) 36 *Forensic Science International: Genetics* 186.

3 Theodore Ruger, 'Health Law's Coherence Anxiety' (2008) 96 *Georgetown Law Journal* 625, 627; Todd Aagaard, 'Environmental Law as a Legal Field: An Inquiry in Legal Taxonomy' (2010) 95 *Cornell Law Review* 221, 229.

4 Michael Guihot, Anne Matthew and Nicolas Suzor, 'Nudging Robots: Innovative Solutions to Regulate Artificial Intelligence' (2017) 20 *Vanderbilt Journal of Entertainment & Technology Law* 385, 452.

5 Arthur Cockfield and Jason Pridmore, 'A Synthetic Theory of Law and Technology' (2007) 8 *Minnesota Journal of Law, Science & Technology* 475.

a jurisprudential and regulatory perspective, it was argued in the literature at that time that a theory of law and technology could provide 'a structure through which lessons learned from technologies of the past can help make decisions about how to regulate and adapt to future technologies'.[6] Technology law is an interesting and dynamic field. As it continues to grow (as it no doubt will), 'coherence in technology law will become clearer and stronger as we continue to study and identify congruencies among the seemingly disparate topics and the complexity of interactions within the field'.[7] Technology law is now an important and much-needed field of study.

> New technologies create novel issues that press at the extremes of the established laws. As has been argued, the established fields of law, weighed down by the requirements of field coherence, are often slow to respond in time or with adequate answers … The speed of change, the rate of change, the novelty of the challenges, the rapidity with which they swamp, not only local markets, but the whole world, and the depth of those changes to our society, our environment, and what it means to be human, makes it necessary to have a set of regulatory responses to new technologies that can, well, respond, in time and at a global level … Technology law must operate where these other laws do not, or cannot adequately. It develops among the interactions between technologies, risks, and their regulation. It works alongside, sometimes with, and sometimes outside of other established areas of law and must be defined accordingly.[8]

It must be noted that in developing a definition of technology law, *technology* is itself a very broad term. What once was considered novel may now be obsolete – and yet it remains a form of technology. Technology is continually evolving across several sub-disciplines such as biotechnology, information technology, artificial intelligence and robotics. There are a number of texts available on information technology, dealing with the law as it relates to computing and the internet. While many areas of technology are closely related to information, either producing it or analysing it, many are not, and this term is too narrow for the burgeoning field that this text seeks to encompass. Defining technology law on the basis of specific areas, such as biotechnology or information technology, would become dated as each developed and morphed into other areas over time. Given the rate of advancement, it is appropriate to approach the subject broadly. For this reason, Donald Schön's definition, outlined in his work *Technology and Change* (1967) has withstood the test of time. This definition of technology encompasses 'any tool or technique, any product or process, any physical equipment or method of doing or making, by which human capability is extended'.[9] In this context, the focus of technology law becomes 'adjusting law and regulation for sociotechnical change'.[10] The complexity of technology is amplified by the pace at which new technologies arise and by the breadth of their impact. Roger Brownsword et al (2017) propose that the unifying question technology law addresses is threefold: first, the

6 Lyria Bennett Moses, 'Why Have a Theory of Law and Technological Change' (2007) 8 *Minnesota Journal of Law, Science & Technology* 589, 605.
7 Michael Guihot, 'Coherence in Technology Law' (2019) 11(2) *Law, Innovation and Technology* (DOI:10.1080/17579961.2019.1665792), 9.
8 Ibid.
9 Donald Schön, *Technology and Change* (Pergamon Press, 1967), 1.
10 Lyria Bennett Moses, 'Regulating in the Face of Sociotechnical Change'. In Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology* (Oxford University Press, 2017), 576.

challenge that new forms of technology pose to 'established legal frameworks, doctrines, and institutions'; second, the 'adequacy of existing regulatory regimes'; and finally, the 'ideas and justifications offered in support of regulatory intervention'.[11]

Recent developments in technology law

Reflecting on political, social and legal developments over the past decade, there have been many relevant issues subject to public debate that engage with technology and law. Briefly highlighting a number of these provides an introduction to the field and is a useful way of foreshadowing the more detailed discussions of these and many other examples that will take place in the following chapters of this text. These examples indicate the balancing act at the heart of many issues in this area of the law – a trade-off between individual and collective rights – specifically, how technology should be used and regulated. The examples are indicative of the need to regulate the harmful aspects of new technology and the associated challenges inherent in doing so, while facilitating the development and adoption of beneficial technological advancements.

While technology has positive and negative applications and implications, recent technological developments can be contrasted with those in the 20th century. Developments such as air travel, the revolution in computing and the discovery of antibiotics all benefited society greatly and, while of course requiring regulation, were associated with relatively few negative implications for most individuals, particularly when considered in the context of the advantages they provided. An exception to this would, of course, be the impact of the Industrial Revolution on the environment and its implications for society; however, further technology has also provided the capacity to mitigate harmful effects of earlier technologies, such as solar and other renewable forms of energy production. In the contemporary examples from the last decade that will be discussed shortly, vast advances in information and communications technology have been associated with compromised privacy and autonomy, principally due to the development of the internet, smartphones, social media, genomics, biometrics and artificial intelligence. Other areas of development where the complex implications of new technology can be observed include healthcare and cybercrime.

Communications

In 2013, a whistleblower from the US intelligence community leaked an enormous amount of information to journalists about the extensive surveillance and analysis of communications, social media and internet usage by the United States and allied countries, including Australia, Canada, New Zealand and the United Kingdom. Edward Snowden, a subcontractor and systems analyst for the National Security Agency (NSA), released classified documents detailing global surveillance programs run by the NSA and the Five Eyes intelligence network, which includes the NSA's partner agencies such as the Australian Signals Directorate (ASD) and the Government Communications Headquarters (GCHQ) in the United Kingdom. It has been estimated that Snowden disclosed approximately 1.7 million intelligence files, including 15 000 Australian files. The disclosures included the names and details of various

11 Roger Brownsword, Eloise Scotford and Karen Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology* (Oxford University Press, 2017), 7–15.

programs run by these agencies. Among them were the *PRISM, XKeyscore* and *Tempora* programs, which enabled 'almost anything done on the internet' to be intercepted, searched and stored by surreptitious tapping of undersea fibre-optic cables and through confidential agreements with technology companies.[12] The documents also revealed that the United States had spied on the communications of world leaders, including several of its allies.[13] A major report commissioned by the US government following these revelations sets out the arguments and counterarguments that might be used to justify these national security activities.

> One of the government's most fundamental responsibilities is to protect this form of security … Appropriately conducted and properly disciplined, surveillance can help to eliminate important national security risks. It has helped to save lives in the past. It will help to do so in the future.[14]

The report also recognises the ethical, as well as potential commercial, implications for the United States of these actions. The discrepancy between what is acknowledged in the report, and the practices that led to it being commissioned, is vast.

> In a free society, public officials should never engage in surveillance in order to punish their political enemies; to restrict freedom of speech or religion; to suppress legitimate criticism and dissent; to help their preferred companies or industries; to provide domestic companies with an unfair competitive advantage; or to benefit or burden members of groups defined in terms of religion, ethnicity, race, and gender.[15]
>
> …
>
> If we are too aggressive in our surveillance policies … we might trigger serious economic repercussions for American businesses, which might lose their share of the world's communications market because of a growing distrust of their capacity to guarantee the privacy of their international users. Recent disclosures have generated considerable concern along these lines.[16]

The countries implicated by Snowden sought to introduce legislation and create a legal framework that supported some of the activities reported, such as metadata retention. Two years later, the Australian government introduced the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth). The Act amended the *Telecommunications (Interception and Access) Act 1979* (Cth), to require telecommunications companies and internet service providers to retain phone, internet and email metadata of all their users for a two-year period. According to the legislation, the content of communications is not stored; however, staff in certain government agencies are able to access the information

12 Glenn Greenwald, 'Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations', *The Guardian*, 11 June 2013. Lina Dencik and Jonathan Cable, 'The Advent of Surveillance Realism: Public Opinion and Activist Responses to the Snowden Leaks' (2017) 11 *International Journal of Communication* 763, 765.
13 Ibid.
14 Richard Clarke et al, *The NSA Report: Liberty and Security in a Changing World* (Princeton University Press, 2014), 1.
15 Ibid, xvii.
16 Ibid, 104.

without a warrant. The legislation states that the content or substance of a communication is not required to be kept,[17] but that all the following information must be recorded:

- the subscribers' accounts, services and telecommunications devices
- the source and destination of a communication
- the date, time and duration of a communication
- the type of communication or service used
- the location of equipment or a line used in a communication.[18]

There is no doubt that telecommunications and internet data can be very important in criminal investigations in understanding the activities of perpetrators and victims, and thus contribute to preventing, investigating and prosecuting serious crime.[19] There are many examples of cases where data retention has enabled the collection of pertinent information that could not otherwise have been accessed; and in the case of the serious and expanding problem of cybercrime, it is the only way offenders can be identified in the real world.[20] The alternate perspective argues that data retention is disproportionate, indiscriminately retaining 'data relating to entire populations, irrespective of the nature of the data or whether or not there is a reasonable suspicion of a serious threat posed by those to whom the data relates'.[21] A further argument that is sometimes overlooked is that the distinction between 'content' and 'metadata' fails to acknowledge how much 'metadata' can reveal about an individual's life, particularly when aggregated and integrated with data analytic programs.[22]

Healthcare

Internet and communications data is not the only area of technology of significance from a legal and regulatory perspective that has advanced rapidly in recent years. The mapping of the genome in 2003, as well as more recent gene editing technologies such as CRISPR/Cas9, have led to a revolution in medical diagnosis and treatment, as well as in reproductive medicine.[23] There are many implications of these new abilities to manipulate DNA. Myriad Genetics is a company providing diagnostic tests that enable doctors to understand the genetic basis of

17 *Telecommunications (Interception and Access) Act 1979* (Cth), s 187A(4).
18 Ibid, s 187AA.
19 Australian Federal Police, *Submission to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 Inquiry by the Parliamentary Joint Committee on Intelligence and Security*. Available: <https://www.aph.gov.au/parliamentary_business/committees/joint/intelligence_and_security/data_retention>.
20 Attorney-General's Department, *Submission to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 Inquiry by the Parliamentary Joint Committee on Intelligence and Security*. Available: <https://www.aph.gov.au/parliamentary_business/committees/joint/intelligence_and_security/data_retention>.
21 Australian Privacy Foundation, *Submission to the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 Inquiry by the Parliamentary Joint Committee on Intelligence and Security*. Available: <https://www.aph.gov.au/parliamentary_business/committees/joint/intelligence_and_security/data_retention>.
22 Even encrypted messages can be accessed. As will be discussed in Chapter 3, the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) compels technology companies to provide police and security agencies with access to encrypted messages.
23 Rodolphe Barrangou and Jennifer Doudna, 'Applications of CRISPR Technologies in Research and Beyond' (2016) 34 *Nature Biotechnology* 933.

diseases, including the risk of development, onset and progression, and optimal treatment strategies.[24] This rapidly growing field of personalised medicine will become increasingly important with the further advances in genomics, enabling therapies that give the individual the best chance of recovery, and gene therapies for major diseases such as cancer. In 1994, Myriad Genetics researchers were involved in research that successfully identified and cloned what is now known as the *breast cancer type 1 susceptibility protein gene* (BRCA1), one of the most significant achievements of modern medical science. Myriad subsequently sought to patent the BRCA1 gene, the part of the human genome that they had been involved in identifying and isolating, an action that was immediately controversial. In the United States, the case *Association for Molecular Pathology v Myriad Genetics Inc* went to the Supreme Court, which ultimately found that it was not able to be patented because '[a] naturally occurring DNA segment is a product of nature and not patent eligible merely because it has been isolated'.[25] Myriad Genetics also sought to patent BRCA1 in Australia, which also resulted in extensive litigation. It was eventually heard by the High Court in the case *D'Arcy v Myriad Genetics Inc*,[26] which reached a similar conclusion and held that the invention was not 'a manner of manufacture' within the meaning of the *Patents Act 1990* (Cth).[27]

Artificial intelligence

The efficiency enabled by new technology is clear, but this can bring its own new problems. An example of this is the way governments and the private sector are now taking full advantage of the efficiencies facilitated by the internet and data analytics in their service provision and business activities. While there are significant efficiency gains to be made, data security remains an ongoing concern, along with other lessons that have been learnt in the first major forays into this area by the Australian government. Automated systems have the potential for efficiency gains in both the private and public sectors that can provide a basis for economic growth. But an understanding of how these systems impact on individual privacy and autonomy must also be taken into account, and is crucial to mitigating the social costs and enhancing the benefits.

One example of the use of new technology in government systems that had a less than ideal outcome was the 2016 Australian Census, subsequently known as #CensusFail.[28] In a process that sought to increase efficiency, the 2016 Census was the first in Australia's history to offer completion of the forms online. However, on census night, 9 August 2016, the Australian Bureau of Statistics' (ABS) system crashed, due to distributed denial-of-service attacks, and was unavailable for citizens to complete their details, making it the most unsuccessful census ever administered by the ABS. It subsequently became known that the ABS shut down the site after it was subject to 'attacks emanating from overseas', which raised questions not only about service provision but data security on the new online platform

24 Myriad Genetics. Available: <www.myriad.com>.
25 133 S Ct 2107 (2013), 2111.
26 (2015) 258 CLR 334.
27 Matthew Rimmer, 'An Exorbitant Monopoly: The High Court of Australia, Myriad Genetics, and Gene Patents'. In Duncan Matthews and Herbert Zech (eds), *Research Handbook on Intellectual Property and the Life Sciences* (Edward Elgar, 2017).
28 Doug Dingwall, 'Bureau of Statistics Looks to Avoid the Mistakes of "Censusfail"', *Sydney Morning Herald*, 16 January 2019.

in comparison with the previous paper-based methods. The Senate inquiry that followed made 16 recommendations for future surveys, including greater scrutiny of the technology that would be deployed for the 2021 Census and prompt reporting of data breaches when identified.[29]

In the social security context, Online Compliance Intervention, otherwise known as 'Robodebt', has caused great controversy in Australia. It relates to the use of data matching systems to compare data from the Australian Taxation Office with welfare payments and income declared to the Centrelink agency, and highlights the unintended consequences that can occur when these systems are introduced to increase efficiency. While efficiency was the primary goal in this case, the automated system actually led to unjust outcomes, negative publicity, a loss of trust in government processes, and increased costs associated with reviews, appeals and interventions.[30]

Social media

While providing important and popular services in internet searching and social networking, it is now well understood that technology companies such as Google and Facebook have become highly profitable and powerful due to the vast amount of data that is provided to them by billions of users around the world and which the companies utilise for advertising purposes. There have been several controversies associated with use of this trove of data; however, the use of Facebook data by the British political consultancy firm Cambridge Analytica in relation to the 2016 presidential election in the United States has received the most coverage. Big data analytics was used in association with information gathered from up to 70 million Facebook users in the United States to develop psychological profiles of voters, which then informed online advertising strategies for the Republican Party. In association with poll results and other intelligence, this strategy was based on the principle that by identifying and understanding individuals in key electorates, different voters could be convinced to have the same opinion on an issue or candidate by using advertisements specifically targeting their personality and social views. The firm was later dissolved after questions arose about the legality of involving a foreign firm in a US presidential election campaign and whether the scale of the activity had compromised the integrity of the election itself. In 2019, Facebook was fined US$5 billion over its management of user data following inquiries into the arrangement.[31]

Cybercrime

Cybercrime is a very significant emerging threat, recently estimated to cost the Australian economy up to A$1 billion annually.[32] It affects government, businesses and individuals, and there are numerous recent examples. In 2019, it was revealed that the Australian National

29 Senate Economics References Committee, *2016 Census: Issues of Trust* (Parliament of Australia, 2017).
30 Senate Community Affairs References Committee, *Design, Scope, Cost-Benefit Analysis, Contracts Awarded and Implementation Associated with the Better Management of the Social Welfare System Initiative* (Parliament of Australia, 2017). Available: <www.aph.gov.au/parliamentary_business/committees/senate/community_affairs/socialwelfaresystem>.
31 Julia Carrie Wong, 'The Cambridge Analytica Scandal Changed the World – But it Didn't Change Facebook', *The Guardian*, 18 March 2019.
32 Australian Criminal Intelligence Commission, *Cybercrime* (2019). Available: <https://www.acic.gov.au/about-crime/crime-types/cybercrime>.

University (ANU) suffered a large and sophisticated cyber attack, losing a large amount of data over a period of several months. The attack targeted a database holding student and staff records relating to a 19-year period. Investigators determined that the details taken included names, addresses, dates of birth, contact details, tax file numbers, payroll information, bank account details and academic records. Information of this type could be of value for identity theft purposes; however, it was speculated that its level of sophistication indicated it was more likely to have been undertaken by a state actor. It has been speculated that China was likely the actor involved and was interested in the ANU's data because of the large number of students who go on to work in government, the foreign service, and Australia's military and security partnerships with the United States, as well as the large number of Chinese students enrolled at the institution.[33] It was the latest in a large number of cybersecurity incidents affecting political organisations, financial institutions and private citizens around the world.

Biometrics

The Identity-Matching Services Bill 2019 (Cth), though not yet enacted, seeks approval for a facial recognition database that integrates images from all passport and driver's licence databases. In addition to a facial image verification service that can be used to prevent identity fraud, a law enforcement database was also introduced. This second database can potentially, and at some point in the future almost certainly will, be integrated with other technologies such as CCTV to allow real-time surveillance in public spaces – an approach that is already widely used in China as part of that country's 'social credit system'.[34] This capability has significant potential for mass surveillance applications and would need to be closely regulated, with developments in China indicating how it could also be used in liberal democracies if safeguards are not implemented. Such developments may already be underway, with Victoria Police confirming that it 'utilises facial recognition technology for investigative and intelligence-gathering purposes across the City of Melbourne council's network of 138 surveillance cameras'.[35]

These are just a sample of some of the areas of technology law that have been discussed in the media over the past decade. They will be explored in greater depth later in the text, following a discussion of regulatory and political theory in Chapter 2. There have, of course, been many more instances, not as widely known, but in their own way just as significant, particularly when trends are considered in aggregate. Technology impacts on so many areas of our lives, it is surprising that it has not yet been given the treatment it deserves in teaching and scholarship.

Whether it is the use of a drone received as a gift, a movie downloaded online, images posted on social media, goods purchased from an online merchant, or research into one's genetic ancestry, the legal implications of new technologies are becoming central to everyday living. Technology will continue to influence not just macro events, such as elections, the implementation of national data systems or advances in biotechnology, but

33 Australian National University, *ANU Releases Detailed Account of Data Breach*, 2 October 2019. Available: <https://www.anu.edu.au/news/all-news/anu-releases-detailed-account-of-data-breach>.
34 Fan Liang et al, 'Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure' (2018) 10 *Policy and Internet* 415.
35 Elias Visontay, 'Councils Tracking Our Faces on the Sly', *The Australian*, 29 August 2019.

everyday transactions that are integral to our lives. To some extent, everyone has an interest in technology law: not just students of law, computer science or criminology; and not just professionals such as lawyers, police, doctors and business owners. Technology is now so integral to everyday life that whatever an individual's background, interests, activities and future intentions, they should have at least a basic understanding of the relevant law.

Overview of the text

The coverage of technology law in this text provides the reader with an accessible and integrated resource for learning and understanding the regulation of some of the most interesting and important issues in contemporary law. It will provide a basic understanding of the technology itself, and act as a guide through the context, relevant policy issues, legislation, case law, international perspectives and gaps in the regulatory framework. The text can be divided roughly into three parts. Chapters 1, 2 and 3 provide background material on technology law, as well as associated theory, regulatory principles and privacy considerations that inform the discussion of all areas of technology law throughout the text. Chapter 2, 'Technology: Regulation and Theory' focuses on epistemic, ethical and regulatory perspectives. It moves from a focused discussion of regulatory theory and the regulation of technology through to the central ethical and political theories, such as social contract, consequentialism and deontology; then to an epistemic discussion of the nature of scientific knowledge; and, finally, to case studies and historical examples of how governments and the legal system have responded to new technology in the past and are likely to respond in the future. Chapter 3, 'Privacy and Data Protection', begins the focus on substantive legislation, common law and human rights instruments. It examines the principles of the law of privacy in Australia, including the *Privacy Act 1988* (Cth) and the Australian Privacy Principles, and provides a comparative discussion of equivalent provisions in the United States, the United Kingdom and Europe. How these provisions interact (or are likely to) with respect to new forms of technology, and the ongoing need to manage the benefits and challenges of technology, particularly with respect to personal information, communications technologies and the internet, are also considered.

Chapters 4–9 consider discrete areas of technology law, with a focus on Australian law, but also drawing on international perspectives. Chapter 4, 'Law, Technology and Healthcare', discusses the regulation of technology used in the healthcare sector. It begins with a contemporary discussion of patient rights and regulatory frameworks, before moving on to consider consent, confidentiality and electronic health records, genetic databases, assisted reproductive technologies, human cloning, gene editing and stem cell technology. Chapter 5, 'Law, Technology and Commercial Transactions', examines the regulation of new technologies that facilitate payments, other financial transactions and contracts. These include online payment systems, cryptocurrencies, blockchain, and the significant and growing problem of online fraud and financial crime, along with approaches to mitigate these concerns. Chapter 6, 'Law, Technology and the Criminal Justice System', considers the use of technology in the criminal justice system. It discusses identification technologies, including fingerprint, DNA and facial recognition systems, which are increasingly important to criminal investigations and related areas such as national security. The use of other technologies such as metadata and automated number plate recognition systems to identify suspects in investigations is also examined. A key theme throughout this chapter will be