Marcus Smith • Seumas Miller

Biometric Identification, Law and Ethics

Springer

Marcus Smith
Charles Sturt University
Canberra, ACT, Australia

Seumas Miller
Charles Sturt University
Canberra, ACT, Australia

TU Delft
Delft, The Netherlands

University of Oxford
Oxford, UK

The research was conducted under the auspices of: (i) the European Research Council's Advanced Grant programme as part of the grant entitled, "Global Terrorism and Collective Moral Responsibility: Redesigning Military, Police and Intelligence Institutions in Liberal Democracies" (GTCMR. No. 670172) (Principal Investigator: Professor Seumas Miller) and (ii) the Australian Research Council's Discovery Grant program as part of the grant entitled, "Intelligence and National Security: Ethics, Efficacy and Accountability" (DP180103439).

ISSN 2211-8101 ISSN 2211-811X (electronic)
SpringerBriefs in Ethics
ISBN 978-3-030-90255-1 ISBN 978-3-030-90256-8 (eBook)
https://doi.org/10.1007/978-3-030-90256-8

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Acknowledgement

The research was conducted under the auspices of: (i) the European Research Council's Advanced Grant program as part of the grant entitled "Global Terrorism and Collective Moral Responsibility: Redesigning Military, Police and Intelligence Institutions in Liberal Democracies" (GTCMR. No. 670172) (Principal Investigator: Professor Seumas Miller) and (ii) the Australian Research Council's Discovery Grant program as part of the grant entitled "Intelligence and National Security: Ethics, Efficacy and Accountability" (DP180103439).

Contents

About the Authors

Marcus Smith is Associate Professor in Law at Charles Sturt University and Adjunct Professor of Law at the University of Canberra. He holds a PhD in law from the Australian National University. He has published widely on technology law, regulation and ethics. His previous books include: *Technology Law* (Cambridge University Press, 2021), *Biometrics, Crime and Security* (Routledge, 2018) and *DNA Evidence in the Australian Legal System* (LexisNexis, 2016).

Seumas Miller has research appointments at Charles Sturt University, TU Delft and the University of Oxford. He is the principal investigator on a European Research Council Advanced Grant on counter-terrorism ethics, and is the author of more than 200 academic articles and 20 books, including *The Ethics of Cybersecurity* (with Terry Bossomaier) (Oxford University Press, 2021) and *Dual Use Science and Technology, Ethics and Weapons of Mass Destruction* (Springer, 2018).

Chapter 4
Biometric and Non-biometric Integration: Dual Use Dilemmas

Abstract Biometric identification is now closely integrated with other forms of data, data systems and communications technologies, such as smartphones, metadata and social media, and as the key security feature on smartphones, and by extension, social media accounts, online profiles and identity. For this reason, we consider the interaction between biometric and other forms of identification data, and data systems, building upon the consideration of the main biometrics in the first three chapters. We begin with a general discussion of data systems and integration. This is followed by a discussion of the interrelationship with biometrics, and broader significance of, metadata, smartphone applications and social media. In combination with biometric identification technologies, these provide detailed insights into individuals' activities and behaviours. The ethical analysis in this chapter focuses on dual use dilemmas. Roughly speaking, dual use dilemmas in science and technology arise in virtue of the fact that such science and technology can be used to greatly benefit humankind, but also, unfortunately, to cause great harm to humankind. Consider, for instance, nuclear science and technology. It can be used as a cheap and peaceful energy source, or to build nuclear weapons. Similarly, facial recognition technology could be used by police only to track persons guilty of serious crimes; or it could be used to monitor ordinary citizens' behaviour by an authoritarian government.

Keywords Biometric identification · Data integration · Big data · Artificial intelligence (AI) · Metadata · Smartphones · Dual use dilemma

4.1 Data Systems and Integration

Over the past 30 years, digitalisation, data analytics and integration has changed the way law enforcement agencies approach criminal investigation, in comparison with traditional information systems –paper-based file and index catalogue systems that required a large amount of storage space, were time consuming to interrogate, and allowed little scope for information sharing outside specific jurisdictions or commands. Just as fingerprint identification moved from manual comparison of ink

M. Smith, S. Miller, *Biometric Identification, Law and Ethics*, SpringerBriefs in Ethics, https://doi.org/10.1007/978-3-030-90256-8_4

prints on cards, to digitalised algorithmic based data systems, so has all other forms of administrative and intelligence data. Similar issues in relation to efficiency, accuracy and data integrity are relevant across these different data systems. Databases are now widely used by law enforcement to store and compare information about crime scenes, individuals and networks. These range from record management systems, to complex analytical software systems that inform tactical and strategic intelligence (Ratcliffe, 2008). While publicly available data on the impact these databases have on investigation outcomes is limited due to sensitivities associated with the nature of the information, there is evidence indicating that these systems can improve policing through the analysis of data, improving the speed of detection, and assisting strategic planning (Koper et al., 2014).

Biometric and other forms of law enforcement data systems have been introduced around the world. In the United States, the Science and Technology Branch of the Federal Bureau of Investigation (FBI) is responsible for the development and maintenance of national police information systems. The Criminal Justice Information System (CJIS) is the central repository of criminal justice information, for the FBI and the other United States federal, state and local law enforcement agencies. United States databases include the National Crime Information Center (NCIC), the National Instant Criminal Background Check System (NICBCS), the Combined DNA Index System (CODIS) and the National Integrated Ballistics Information Network (NIBIN) (Federal Bureau of Investigation, 2021).

In the United Kingdom, the Home Office and the Association for Police and Crime Commissioners manage Britain's police information systems. Current databases include the Police National Database (PND), the Police National Computer (PNC), the National DNA Database (NDNAD), the National fingerprint and identity platform database (IDENT1), and the National Ballistics Intelligence Services (NABIS).

The Australian Criminal Intelligence Commission (ACIC) was formed in 2016 following a merge between the Australian Crime Commission (ACC) and the CrimTrac Agency. CrimTrac had been responsible for the development, sharing and maintenance of law enforcement databases in Australia since July, 2000, while the ACC was the a federal agency established to investigate organised crime. According to the ACIC, its databases seek to enhance Australian policing and law enforcement, and '…contribute directly to the effectiveness and efficiency of police and law enforcement agencies in Australia' (ACIC, 2021). In addition to DNA and fingerprints, the ACIC administers national databases relating to ballistics, cybercrime reports, firearms ownership, vehicles and persons of interest (ACIC, 2021).

A range of issues can impact the effectiveness of police information systems such as poor implementation and underutilisation of the databases, as well as a lack of training. Data security, missing or inaccurate data (completeness and validity), siloed information, ineffective human-computer interfaces, poor search capabilities and hardware limits need to be considered and managed when implementing new information systems into police agencies and practices (Koper et al., 2014).

As its potential to solve complex problems efficiently becomes increasingly apparent, law enforcement and intelligence agencies are collecting and analysing an increasing volume of data about individuals, in order to prevent and investigate crime. Big data analytics uses tools, techniques and technologies to store, manage and efficiently process this expanding amount and range of data currently being generated. It is characterised by features such as volume, velocity and variety (Pramanik et al., 2017). Identifying the network structures of criminals and inferring their roles can assist law enforcement and intelligence agencies to prevent crime. This can be achieved by mining social media data from sites such as Facebook (which as discussed in Chap. 2, can include biometric facial templates) (Tan et al., 2013). Because it is likely that criminal activities will become increasingly digitised, law enforcement and security agencies are expanding their use of data mining techniques. The proliferation of digitalised data means that it is possible to merge diverse data sets into integrated systems, to enable cross referencing and searching. In contrast, with the previous approach, requiring officers to individually search 'siloed' databases of criminal history, car licence plates etc., intelligence analysts can now interrogate one integrated system that integrates disparate data sources:

> This integration facilitates one of the most transformative features of the big data landscape: the creep of criminal justice surveillance into other, non–criminal justice institutions. Function creep – the phenomenon of data originally collected for one purpose being used for another – contributes to a substantial increase in the data police have access to. Indeed, law enforcement is following an institutional data imperative, securing routine access to a wide range of data on everyday activities from non-police databases (Brayne, 2017).

Palantir is one example of a private sector data integration platform widely used by law enforcement and intelligence agencies around the world. It provides for a tagging system that enables users to visualise and map data, by labelling and linking persons, objects and entities, such as phone numbers, cars, photos, email addresses, social media accounts, metadata, biometric database profiles, and intelligence reports, establishing inter-relationships. Another example is the Enterprise Master Person Index (EMPI), developed by Los Angeles County, that links an individual's interactions with social security, healthcare and law enforcement agencies in order to improve government service delivery (Brayne, 2017).

There are a number of challenges associated with the increasing utilisation and integration of data, and the first point that should be noted is data security. New approaches to consent, management and data protection may be needed to deal with the rapid expansion in the volume and type of data available, and the myriad ways in which it is being used (Kaye et al., 2015). Cases of hacking and significant data breaches involving institutions, governments and businesses are becoming more common (ANU, 2019). The capacity to integrate biometrics, metadata, financial, medical and tax data, adds to these concerns. The use of identification technologies in China to construct a social credit system (discussed further in Chap. 5), demonstrate a potential development of biometric and other data integration in liberal democracies, absent appropriate regulation.

Biometric technologies are an important part of a broader shift taking place in society towards automated decision-making processes that involve more limited

human intervention. Artificial intelligence (AI) and deep learning (DL) algorithms are rapidly becoming an important application in relation to biometric data, and a range of other fields, including clinical medicine, finance and government administration. AI refers to computer systems that perform tasks traditionally associated with human intelligence. The algorithms recognise patterns, conduct abstract reasoning and learn from prior examples to undertake pattern recognition tasks (Smith & Heath Jeffery, 2020). There are challenges associated with implementing AI systems in any field because it is not possible to understand precisely how an algorithm arrives at a particular conclusion – described as the problem of black box data processing. Human decision making is complex and often requires contextual knowledge and experience. Continued human oversight is crucial in verifying the accuracy and safety of AI applications in order to facilitate their integration over time. Further, quality standards for implementation, and ensuring AI data is continually evaluated as part of the decision-making process, will be important in preventing and mitigating potential errors. Moreover, from a legal perspective, who will be responsible for errors that occur with the application of AI technology remains unclear. As regulation is developed, it will need to be determined to what extent humans that oversee the technology; institutions that use the software; and the algorithm developers will bear liability. Given the complexity of AI technology, determining where the error occurred, and who is responsible, may be difficult to ascertain.

The challenge of regulating biometric data is part of a broader issue of technology regulation. New technology offers great potential for efficiencies and economic growth, but complex problems associated with privacy, accuracy and data security is an ongoing concern. Effective technology regulation requires an understanding of the relevant science and what the implications are for the individual and society; ethics and regulatory theory, to determine why it should be regulated; and an understanding of legal and parliamentary processes, to determine how it should be regulated. Technology is continually adapting, advancing, and being integrated with new capabilities and applications. Holistic approaches to technology regulation, across a number of sectors, rather than siloed approaches will be most effective over time.

Government agencies today have much greater powers to collect evidence and conduct surveillance to detect and disrupt threats like terrorism and transnational crime (Walsh & Miller, 2016). More proactive collection of data, including biometric information, from citizens who have not committed a crime has become increasingly common, –facilitated by the exponential increase in data created by consumers of services provided by technology and social media companies.

4.1.1 Metadata

Metadata is data that provides information about, or describes, other data. For example, metadata about a text message, may include the phone numbers and type of phones it was sent and received from, their location, and the time and date it was sent–but not the content of the text message itself (Sarre, 2017). The advent of

smartphones, which today individuals carry on their person almost everywhere, vastly increased the availability of metadata. Biometrics, in providing access to smartphones, are intrinsically linked to this metadata. Metadata generated by smartphones and internet activity is collected by technology companies for advertising purposes, and many liberal democratic countries now require it to be retained for several years in case it is required in a law enforcement investigation. It is arguably the most significant other form of identification technology at the present time in terms of providing insights into individuals' lives. Integrating metadata with the biometrics discussed throughout this text: biometric data used by technology companies (e.g., facial image access to devices or services); government service provision (e.g., CCTV, passports); and law enforcement (e.g., DNA evidence and facial recognition) allows a very thorough picture of an individual's identity and daily activity can be achieved. The scope of this continues to expand as new devices and applications become available (Sarre, 2017).

The use of metadata and social media by governments was at the heart of Snowden leaks in 2013 (Walsh & Miller, 2016). These leaks provided details of global surveillance programs run by the National Security Agency in the United States, and the Five Eyes intelligence network that collected 'almost anything done on the internet' through confidential agreements with technology companies (Dencik & Cable, 2017). In the time that has passed since, many countries have passed legislation that requires technology companies to store metadata for a number of years and provide it to government agencies if it is deemed necessary for a law enforcement investigation.[1] Some countries have even legislated to prevent encryption hindering law enforcement agencies from accessing metadata.[2]

Australian legislation introduced in 2017 provides a useful example of laws that were introduced following the Snowden leaks.[3] These state that, while a warrant is necessary to obtain the content of communications, metadata can be accessed without a warrant if it is deemed reasonably necessary for an investigation. Telecommunications service providers are required to retain Australian's metadata for two years in order to ensure that it is available for law enforcement investigations if required.[4]

The legislation that facilitates metadata retention is the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth). It came into effect in October 2015, with telecommunication service providers given until April

[1] E.g. in Australia, the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) gave telecommunication service providers given until 2017 to establish infrastructure to retain customers' metadata. Section 172 of the legislation states that disclosure of 'the contents or substance of a communication' is not permitted. Details of the kinds of metadata telecommunications service providers are required to retain are provided in section 187AA of the legislation.

[2] Australia enacted (world first legislation) the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act* 2018 (Cth).

[3] *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth).

[4] Ibid, section 172.

2017 to develop infrastructure to retain customers' metadata for the two year period and deliver it to government agencies upon request. While section 187AA of the legislation defines metadata, one aspect that the legislation is unclear on is whether the URLs of websites visited when browsing the internet are considered metadata, which remains unresolved:

> …metadata (in the context of web browsing) is what remains of a communication or document after its contents and substance is excluded. As a result, the legal definition of metadata is ambiguous; an oversight commentators suggest is surprising. In part, the ambiguity arises from conflicting views on what constitutes 'the content' of a communication. For example, one of the most contentious issues of the current Australian regime is whether URLs are metadata. If they are, then warrantless governmental access to individuals' web browsing history is possible. One view is that as URLs are user-generated, they are content. Another view – expressed by the Attorney-General's Department – is that metadata is 'information that allows a communication to occur'. As that is what URLs do, consequently they are not content. The issue is that that some URLs can identify the substance of a communication (Murphy, 2014).

In Australia, metadata can be accessed without a warrant and there is a relatively low threshold for access. There is only a requirement that it be reasonable necessary for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue.[5] It appears that in the years since the metadata legislation was introduced, the number of requests to access it increase each year, as well as the number of government agencies that are permitted to access it. While this type of legislation is passed with politicians discussing the threat of terrorism and its need in that context, over time it is clear that comprises a small proportion of the types of investigations for which it is being used (Redrup, 2019).

Law enforcement may be able to access full content of data held on smartphones with a warrant; however, their ability to do so may be constrained by technical capability i.e. through encryption. A high-profile example of this occurred in the United States in 2016. Apple was ordered by a federal court to 'assist law enforcement agents in enabling the search' of an iPhone seized in relation to a shooting in San Bernardino, California, by unlocking it (Pollack, 2019).[6] Apple resisted this request and publicised the issue, with the CEO Tim Cook declaring the company's opposition and calling for public discussion of the issue of data security. Apple argued that creating a back door into their phone system would weaken their security system for all users, and refused. It was later revealed that the FBI used an Australian firm Azimuth, to break the encryption and access the phone (Nakashima & Albergotti, 2021).

[5] Section 179(3).

[6] Order Compelling Apple, Inc to Assist Agents in Search, In re Search of an Apple iPhone Seized during Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203, No 15-0451, *1 (CD Cal filed Feb 16, 2016) cited in Michael C. Pollack, 'Taking Data' (2019) 86 *University of Chicago Law Review* 77

Australia has enacted legislation facilitating access by law enforcement and national security agencies to encrypted content.[7] This was controversial, although encryption can be used by criminals to communicate and carry out crime, and prevent law enforcement agencies from investigating them or obtaining evidence, it also has legitimate uses, such as securing financial transactions and protected communications (such as between a lawyer and their client). The *Telecommunications and Other Legislation Amendment (Assistance and Access) Act* 2018 (Cth) requires technology companies to provide reasonable assistance to access the content of communications facilitated by their platforms. Under the legislation, technology companies may be required to respond to the following:

- A technical assistance request (TAR): a request that they voluntarily assist law enforcement by providing the technical details about one of their products or services;
- A technical assistance notice (TAN): a requirement that they assist by decrypting a specific communication, or face a fine if they refuse; or
- A technical capability notice (TCN): a requirement that they create a new function to enable police to access a suspect's data, or face a fine if they refuse.[8]

Decision-makers must be satisfied that the request or requirement is reasonable and proportionate and that compliance is practicable and technically feasible.[9] In addition to privacy issues, stakeholders in the technology industry are concerned that creating vulnerabilities in their systems that would compromise their ability to provide their services to their customers, and impact on the commercial viability of Australian companies in the international marketplace. While the legislation was amended to expressly provide that companies 'must not be requested or required to implement or build a systemic weakness or systemic vulnerability';[10] there remain concerns in the technology sector and community about these laws.[11]

A law enforcement operation to access encrypted smartphone communications between 2018 and 2021, led by the FBI and Australian Federal Police, was recently revealed. The Trojan Shield/Operation Ironside operation involved police developing an 'encrypted' messaging app, called ANOM, and marketing this to organised crime groups via undercover agents. The app had a back door that could be accessed by law enforcement and provided a wealth of information and understanding of criminal networks over several years, before being revealed in 2021 and leading to the arrest of more than 800 people worldwide (Pannett & Birnbaum, 2021). This

[7] Encryption is the process of encoding messages so that their content can only be read by those that send and receive them.

[8] Defined in *Telecommunications and Other Legislation Amendment (Assistance and Access) Act* 2018 (Cth), section 317B.

[9] Section 317JAA (TARs); section 317P (TANs); and section 317TAAA(6) (TCNs).

[10] Section 317ZG.

[11] *Questions on Notice from Senetas Corporation*, Parliamentary Joint Committee on Intelligence and Security, Review of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 (Parliament of Australia, 2018).

development highlights the increasing sophistication and audacity on the part of law enforcement agencies to access communications data that they believe is relevant to investigations, and prevent technology from being used to facilitate organised crime.

4.1.2 Smartphone Applications

Fingerprint and facial recognition biometrics are now widely used to identify and grant access to a smartphone. Due to the high level of security these biometrics provide, possession of a smartphone registered to a specific person has become a proxy for the identity or location of that person (Smith & Urbas, 2021). For example, a smartphone can now be used as a tap and pay device, in the same way as a credit or debit card has been used in the past, it can be used to record the presence of a person at a location, using quick response (QR) code scanning, and provides access to social media and other online accounts.

The accuracy and security of biometric identification technologies have enabled smartphones to become an extension of the physical self for identification purposes. This development was widely observed in relation to government responses to the COVID-19 pandemic. This significant threat to public health, the economy and national security around the world, in 2020 alone, it infected more than 60 million people worldwide, and killed more than 1.5 million (WHO, 2020). Governments adapted existing technologies to inform decision making and improve contact tracing of those who contracted COVID-19 in order to limit the spread of the disease. A range of surveillance technologies can potentially assist with contact tracing, including closed-circuit television cameras, facial recognition technology, thermal imaging cameras, location metadata, automated numberplate recognition and financial transaction data (Servick, 2020).

Given the wide use of smartphones, several countries used metadata to geolocate individuals, while others developed specific apps that the population was required to download which communicate with surrounding phones via Bluetooth, in order to identify other persons that an infected individual has been in close contact with. Technology applications generate information to inform the community and allow them to make decisions that reduce their chance of contracting the virus. This can be an alternative to, or used in conjunction with, lockdowns and curfews, to prevent community transmission of the virus. In both cases, it was argued that the seriousness of the pandemic overrode individual autonomy rights. In South Korea metadata tracking was used to inform community announcements about the movements of individuals who had contracted the virus. The government actually published anonymised maps of the locations those who had contracted COVID-19 visited (Servick, 2020).

China was the country of origin for COVID-19 as well as being the leader in public surveillance (Wang, 2020). As will be discussed further in the following chapter, China has established a social credit system that uses big data integration to profile citizens, and impose sanctions if they repeatedly fail to comply with

government policies. The country was well placed to implement technology based public health surveillance systems. The Chinese smartphone application that was introduced in response to the COVID-19 pandemic was known as *Health Code*, and available via the Alipay and WeChat platforms. The application has be described as follows:

> People first fill in their personal information, including their ID number, where they live, whether they have been with people carrying the virus, and their symptoms. The app then churns out one of three colors: green means they can go anywhere, yellow and red mean seven and 14 days of quarantine, respectively. The app also surreptitiously collects – and shares with the police – people's location data (Wang, 2020).

The application has more than 700 million users, who are required to show the colour it displays when they, for example, enter residential areas, shopping centres or public transport, and verify their identity with facial recognition technology. An issue that has caused some debate in China, is that the algorithm that determines the colour allocation has not been disclosed, so individuals do not know what has caused them to receive a yellow or red rating, with those affected criticising this as being ruled by machines (Wang, 2020). There have also been indications that the application will remain in place after the pandemic has ended, for ongoing public health monitoring and health care service provision, further expanding the already extensive government surveillance infrastructure (Sheng & Zijia, 2020).

Bluetooth technology does not monitor an individual's location and applications of this type have been introduced by governments in Australia, Singapore, among others, and have been largely accepted in those countries, although ultimately proved not to be effective for contact tracing purposes and were replaced with other measures, such as QR code scanning upon entry to locations such as shops and workplaces (Bogle, 2020). Metadata based COVID-19 contract tracing has been more controversial – it can track a person's location whenever their phone is in their possession.[12] In addition to South Korea, metadata has also been used in Israel, where it was reported that a database of citizens' metadata compiled by security agency Shin Bet was being used for contact tracing purposes (Halbfinger et al., 2020). In Norway, the COVID-19 tracing application, *Smittestopp*, which utilised metadata and Bluetooth technology, was criticised by the national data protection agency for its impact on privacy and ultimately suspended (Guardian, 2020).

Security threats are used by governments to make effective claims about necessary measures to address the threats and take exceptional actions beyond what would normally be acceptable (Williams, 2003). As was also relevant to the metadata discussion, the security rationale used in relation to COVID-19 has been repeated used in the past (e.g., counter terrorism), to introduce more extensive data collection practices and associated legislation. There is potential for the collection of data for public health purposes to continue after the threat has passed as part of an ongoing preventative, just as measures to combat the heightened risk of terrorism

[12] As noted above, metadata refers to information such as the location of the devices used, the phone numbers involved in a communication, and the date and time of the communication.

after 9/11 became later employed against serious crime, and then against less serious crime. Metadata collection expanded from initially being used by only select law enforcement and security agencies to being used more widely across government (Smith & Urbas, 2021). Function creep is an important issue to consider in relation to identification technology regulation. Democratic governments should ensure that data is collected for a specific purpose, particularly where it is undertaken in response to extraordinary circumstances such as 9/11 or COVID-19, it is vital that it not used for purposes beyond those intended when the laws were enacted. The technology sector is rapidly growing, with new applications becoming available each year. Potential outcomes of unchecked use of surveillance technologies in liberal democracies is illustrated by the extensive data systems established in China, and in particular their use in relation to ethnic minorities.

4.1.3 Social Media

As noted above, biometric fingerprint and facial recognition, in regulating access to smartphones, simultaneously provide access to social media accounts, and are therefore key indicators of a person's identity in online environments. Facial recognition is widely used to identify and link individuals within social media platforms, such as Facebook's tagging feature (Smith & Urbas, 2021). Biometrics are therefore closely associated with the developments in social media that have significantly influenced the society over the past decade, and they will continue to be central as these applications continue to expand, as well as to future regulatory approaches.

Social media does not include all online websites, but involves a degree of interaction between participants, and collaboration in a non-hierarchical way. It enables users to post self-generated content, such as text and photos; allows users to create profiles and engage with others by posting comments or 'likes'; and, enables users to network with others that hold similar interests or opinions (Obar & Wildman, 2015).

Technology companies such as Google and Facebook have become powerful due to the vast amount of data they holding detailing the internet activity of their billions of users (De Zwart et al., 2014). How information available on the internet is presented to users also has a significant capacity to influence social views and trends. In contrast with traditional mediums, there is a relative lack of central control over content that can facilitate mistruths to be perpetuated.

It has recently been proposed in a number of countries around the world, that social media users must provide evidence of their identity, such as a copy of a passport or drivers licence in order to obtain, or maintain a social media account (Australian Parliament, 2021). The objective of this approach is to address the issue of people using anonymous accounts to harass and abuse online: described as 'technology facilitated abuse', or commit other crimes.[13] In an anonymous online

[13] Ibid, Recommendation 30.

environment, vitriolic comments can be widely observed on public social media websites. Online harassment may target individuals or groups on the basis of race, ethnicity, religion or sexual orientation, and is widespread, with recent survey data indicating that one in three have experienced some form of online harassment impacting their health, safety and productivity (Australia Institute, 2019).

There are other issues arising from social media that may also be mitigated with the introduction of identity verification measures. The dissemination of misleading or inaccurate information or theories, commonly referred to as 'fake news', that can rely on automated dissemination using botnets: such as misinformation (conspiracy theories and pseudoscientific therapies) in relation to the COVID-19 pandemic (Naeem, 2020). The efficiency with which social media can disseminate information was highlighted (in association with big data analytics) by the former consultancy firm Cambridge Analytica's online advertising strategies for the Republican Party in the 2016 presidential election campaign. In association with poll results and other intelligence, the firm sought to identify and understand individuals in key electorates, then use social media advertisements specifically targeting their personality and social views to influence their vote (Wong, 2019).[14] These and other developments over recent years, along with the extent to which it is now used around the world, means that social media can significantly impact the lives of individuals and the nature of society. There is an argument that 'social media is too powerful now to be anonymous' and that just as identification and registration is required to drive a car or own a firearm, so it should also be required to operate a social media account (Burns, 2018).

To date, laws requiring compulsory identity verification for social media account holders have not been introduced. They could plausibly deter online harassment and abuse, hate speech and disinformation and enable it to be better investigated and prosecuted. However, there are some potential issues with the approach that should be noted. For example, data security, if identity documents, such as copies of passports and drivers licences, were provided to multinational technology companies such as Google and Facebook, which already have a great deal of personal data about users online and real world (e.g. location metadata) behaviour, they would be a target for organised crime groups, and would increase the level of risk associated with the already detailed and sensitive information that social media companies hold about individuals. There would need to be confidence that this risk could be adequately mitigated before implementation (Druce, 2021).

[14] The firm was later dissolved after criticism about the legality of hiring the firm for the presidential campaign in light of prohibitions on the involvement of foreign citizens in United States election campaigns 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.

4.2 Ethical Analysis

In earlier chapters on specific biometrics, namely, fingerprinting, facial recognition technology and DNA, we discussed a number of (often recurring) ethical or moral problems. Central among these was the conflict between individual (including joint (Miller, 2003)) rights to privacy/autonomy/ownership of biometric data, on the one hand, and the collective good of security (Miller, 2010 Ch. 2), on the other hand. Provision of the collective good of security via, for instance, databases of fingerprints, facial images or DNA, was framed as a collective (understood as joint) moral responsibility (Miller, 2006, 2010 Ch. 4). On the other hand since, as we argued, there were moral costs associated with the creation of these databases and, in particular, the infringement of individual rights to privacy and/or autonomy and/or ownership of biometric data, there was a requirement to engage in ethical analysis with a view to accommodating these individual rights in the context of pursuing the collective good of security.

In this chapter, by contrast with earlier chapters, we have described a plethora of interconnected indeed, in many cases, integrated biometric and non-biometric technologies, including databases and associated analytics, smartphone and other applications, encryption and so on. Each of these developments calls for ethical analysis in a piecemeal fashion, but we cannot embark on these analyses in any detail here. For these analyses would take us well beyond our specific focus on biometrics, even if space limitations permitted which they do not. However, we suggest that most of these developments, whether taken singly or in totality, involve a conflict between individual rights and collective goods and, as such, the ethical machinery developed in earlier chapters remains relevant to the required ethical analyses. For instance, the use of metadata by law enforcement and national security, and of smartphone applications for contact tracing in combating COVID 19 can be framed in this manner, or so we have argued elsewhere (Miller & Smith, 2021). Again, the integration of biometric databases (e.g. fingerprint, facial image and DNA databases) with non-biometric databases (e.g. financial or health databases) could greatly facilitate law enforcement and, thereby, increase the collective good of security (Miller, 2010 Ch. 2), but would do so at some (potentially unacceptable) moral cost in terms of infringements, if not violations, of individual rights, as the Snowden revelations (Miller & Walsh, 2016) demonstrated (see the following chapter for more on this issue). Moreover, the existence of these databases is not simply an unalloyed security benefit, since databases give rise to data security concerns in the first instance, and indirectly other wider security concerns, including law enforcement and national security concerns (Miller & Walsh, 2016; Miller & Bossomaier, 2021). For instance, databases can be hacked, and personal and confidential data compromised (including the data of law enforcement or national security agencies). Databases can also be encrypted by malevolent actors for purposes of blackmail i.e. so-called ransomware attacks, e.g. on the National Health Service in the UK. Favoured targets here include hospitals and other organisations whose data is relied upon for health purposes, including to save lives.

Other specific issues with a biometrics aspect, such as encryption and social media touched on above, also implicate privacy and autonomy rights in ways that problematize any easy framing of the ethical issues in terms of individual rights versus collective goods (Miller, 2003, 2010 Ch. 12 Sec. 2). For instance, end-to-end encryption has greatly assisted criminal organisations and thwarted law enforcement, as well as ensuring the privacy of the communications of ordinary law-abiding citizens. Arguably, therefore, citizens do not have a moral right to end-to-end encryption as libertarians are inclined to believe. Again, social media has enabled the proliferation of harmful false hoods (e.g. fake news, and ideology) and thereby demonstrated what should have been obvious, namely, that there is no *unqualified* right to free speech (Miller, 2020). At any rate, social media is in need of regulation, but the ethical issues in this area are very complex and cannot simply be framed in terms of individual rights versus collective goods (albeit this is an important dimension of the moral problem) (Miller & Bossomaier, 2021).

We suggest that in addition to piecemeal analyses of these ethical problems there is a need to take a bird's eye view and consider, in particular, the extent to which these various technologically-based developments have created unacceptable power imbalances between the citizenry on the one hand, and the state on the other (and perhaps, also, between the citizenry and large corporations). The general issue here is that of the potential to undermine fundamental tenets of liberal democracy. We discuss this issue in more detail in the following chapter.

We also suggest that most of these developments, whether taken singly or in totality, involve what is referred to in the literature, and as foreshadowed above, as dual use ethical dilemmas (Miller & Selgelid, 2007; Rappert & Selgelid, 2013; Miller, 2018). We suggest that the notion of dual use ethical dilemmas can usefully frame and elucidate many of the overarching ethical issues that arise from the use in law enforcement and national security contexts of biometrics and, especially, the integration of biometric and non-biometric technologies. This is essentially because although the use of biometrics integrated with non-biometrics can bring great benefits in terms of security it can also impose great moral costs. These moral costs connect the problem of dual use dilemmas to that of concerns about liberal democracy. For, as we will see in the next chapter, the great moral costs in question are dramatically evidenced in the use of these technologies in authoritarian states, such as China, to control the citizenry but also, at least potentially, in those liberal democracies which use these technologies in unacceptable ways or without adequate safeguards. Let us now turn to a more detailed account of dual use dilemmas.

4.2.1 Dual Use Ethical Dilemmas

Dual use technology can be considered a single technology with a dual use or as two (or more) technologies which in combination have a dual use. Thus, research on the transmissibility of a pathogen undertaken in a secure laboratory for the purpose of developing a vaccine might be (potentially) hugely beneficial to humankind.

However, since such research might involve the production of a more transmissible form of the pathogen in question it could also enable a malevolent actor with biological training, such as an 'end-of-the-world' terrorist, to deliberately cause a hugely harmful pandemic (Miller & Selgelid, 2007; Rappert & Selgelid, 2013; Miller, 2018 Ch. 8). This example is an instance of a single type of scientific research having a dual use. Now consider facial recognition technology integrated with CCTV camera technology to enable the tracking of individuals. This integrated combination of technologies is dual use in that it could be used by police only to track persons guilty (or, at least, reasonably suspected of being guilty) of serious crimes (Miller & Gordon, 2014) i.e. it is used only for necessary and legitimate law enforcement; or it could be used to monitor ordinary citizens' behaviour in order to ensure their compliance with the human rights-violating dictates of an authoritarian government.

Our main focus in this chapter is with dual use ethical dilemmas arising from the integration of biometric and non-biometric technologies i.e. with biometric and non-biometric technologies taken in combination. Our reason for doing so is that dual use ethical dilemmas in biometrics arise in their most acute form when biometrics are integrated with non-biometric technologies, such as facial recognition technology with CCTV camera technology, or biometric databases integrated with non-biometric databases and associated analytics, such as facial image databases of known persons (e.g. derived from passport photos) integrated with phone metadata databases, social security databases, social media data mined from social media sites etc. potentially enabling the development of profiles of particular individuals suspected of crimes but also potentially enabling authoritarian states to monitor and suppress their populations; or, in the case of private companies, to develop customer profiles for the potential purpose of better meeting their needs but also potentially enabling large-scale manipulation of customers to enhance the profits of companies (Zuboff, 2019). Another general area of concern here might be the interlinking not only of biometric and non-biometric databases and use of associated analytics, such as data mining or machine learning techniques (Miller & Bossomaier, 2021), but also the interlinking of government and private sector held databases (of which more below).

The problem of dual-use ethical dilemmas in relation to powerful, new and emerging technologies, including biometrics integrated with non-biometrics, arises because such technologies have the potential to be used for great harm as well as for great good (See e.g. Miller & Selgelid, 2007; Rappert & Selgelid, 2013; Meier & Hunger, 2014; Miller, 2018). On the one hand, such technologies can contribute greatly to individual and collective well-being. Consider, for example, nuclear technology that enables the generation of low cost electricity in populations without obvious alternative energy sources. So, as mentioned above, nuclear technology is a good thing. On the other hand, these same technologies can be extremely harmful to individuals and collectives. Consider, for example, the atomic bombs dropped on Hiroshima and Nagasaki. So it seems that some powerful technologies or, at least, some uses of some powerful technologies, are a bad thing and, therefore, knowledge of these technologies is a bad thing and ignorance a good thing. Accordingly, the question arises as to whether we ought to limit the development of these

technologies or, more likely, restrict the uses of these technologies and, in particular, the proliferation of these technologies and perhaps dissemination of the knowledge how to develop them (assuming this is possible).

By definition, dual use technologies are potentially harmful as well as beneficial, and therefore, there is a need to limit these technologies, or their uses, in a manner that decreases the risk of harm while preserving the benefits. In relation to the potential for harm, governments, regulators, scientists, designers and manufacturers technology and, in the cases of interest to us, law enforcement and national security agencies who use the technology, have a moral responsibility and, specifically a collective or joint moral responsibility. This is so, even if there is not at present a legal responsibility, to cooperate in order to avert or, at least, minimise the risks. Dual use research and technology is a matter of *collective moral responsibility* to avert or minimise harm (Miller, 2018 Ch. 4). But how does collective responsibility figure in the various scientific, technological and institutional contexts in question? More specifically, should some dual use research and technologies be impermissible or, if not, should certain uses of these technologies be curtailed? For instance, in some jurisdiction in US and in the EU, certain uses of facial recognition technology have been banned. More generally, what institutional arrangements, e.g. regulations, ought to be put in place in relation to dual use biometric technologies and uses thereof, specifically in the context of this work by security agencies?

"Dual use" refers to scientific research or technology that can be used for both beneficial/good and harmful/bad purposes (See e.g. Miller & Selgelid, 2007; Miller, 2013, 2018; Meier & Hunger, 2014; Tucker, 2012). However, this general sense of dual use is too broad since it has the effect that almost everything could count as dual use. For instance, machetes are used for farming, but they were also used in the Rwandan genocide in 1994 as tools of murder. So we require a narrower notion of dual use. Most of the current debate has focused on research and technologies with implications not simply for weapons but for weapons of mass destruction (WMDs), in particular – i.e., where the harmful consequences of malevolent use would be on an extremely large scale (Miller, 2018). That said, defining dual use simply in terms of WMDs yields too narrow a notion given, for instance, the possibility of creating de novo new pathogens which are both highly virulent and highly transmissible (NSABB, 2015; Selgelid, 2016). Moreover, the biometric technologies of interest to us in this work do not have any obvious implications for WMDs, yet they are potentially able to cause serious harms on a very large scale in the hands, for instance, of authoritarian governments. Accordingly, let us try to get a better fix on a serviceable notion of dual use by setting out a number of different preliminary definitions of dual use familiar in the literature and doing so on the assumption that any definition will involve a degree of stipulation (Miller & Selgelid, 2007; Miller, 2018 Ch. 1).

Research or technology is dual use if it can be used for both:

1. Military and civilian (i.e. non-military) purposes; or
2. Beneficial and harmful purposes – where the harmful purposes are to be realised by means of WMDs; or

3. Beneficial and harmful purposes – where either the harmful purposes involve the use of weapons as means, and usually WMDs in particular, or the large-scale harm aimed at does not necessarily involve weapons or weaponisation[15].

We favour the third definition of "dual use" since some dual use research, such as gain-of-function research in the biological sciences, or research in biometrics leading to the increasing sophistication of facial recognition technology or the integration of biometric and non-biometric databases (and use of associated data analytics), need not involve an explicit process of weaponisation or a military purpose. Moreover, whereas biometrics can assist in the realisation of military purposes, e.g. facial recognition technology used on predator drones to identify nominated human targets to be killed: facial recognition technology is not a weapon per se.

Dual-use refers to two conceptually distinct groups of actors[16]: (i) those who initially undertake the research and/or develop the technology (let us refer to these as original researchers/developers); and (ii) those who use the results of the work of these original researchers/developers, e.g. security agencies. In the case of dual use technologies, the original researchers/developers presumably designed the technology with the intention that it be used for beneficial purposes, even if they were aware that it could also be used for harmful purposes. The general point being that their intention was not that it be exclusively or predominantly used for harmful purposes, as in the case of weapons technology. That said, dual use technologies are, to reiterate, technologies that could be used for harmful purposes and it is certainly possible that dual use technologies were designed to be used for both beneficial as well as harmful purposes.

In relation to the term, "use", we can distinguish: (i) actually or potentially used in accordance with the purpose for which it was designed (design-purpose); (ii) actually or potentially used for some purpose other than that for which it was specifically designed; (iii) actually or potentially used for a benevolent and, therefore let us assume , morally good purpose; (iv) actually or potentially used for a malevolent and, therefore, morally bad purpose.[17] Dual-use dilemmas typically involve: (A) original researchers/developers undertaking scientific research or developing technology for a good purpose – the design-purpose is good; and (B) malevolent secondary (actual or potential) users – the research is to be used to cause great harm. This is consistent with their being some other group of original researchers who had a malevolent design-purpose. However, on our definition of dual use there needs to

[15] There is a distinction between an object which is a weapon merely because used as one, e.g. a brick used to hit someone on the head, and a weapon which was designed as such from material which is not in itself useable as a weapon and, therefore, needs to go through a process of weaponisation, e.g. a biological agent used in a bioweapon.

[16] Two things can be conceptually distinct even if under some description they are the same thing. Thus being married is conceptually distinct from being a scientist. However, Jones can be a married scientist. Similarly, the original researcher could also be the secondary user, notwithstanding that original researcher and secondary user are distinct concepts.

[17] We are assuming that in the final analysis the dual use dilemma is a moral dilemma and, therefore, the harms and benefits in question are morally significant (either directly or indirectly).

be a group of original researchers who have a good purpose (even if they designed the technology is a manner that enable it also to be used for a bad purpose). This good purpose is either a good design-purpose or a morally neutral design-purpose which is a means to some further good purpose that they have.

Consider facial recognition technology. It was designed, obviously, to enable people to be identified by use of facial images. Accordingly, in the hands of appropriately regulated law enforcement agencies in a liberal democratic state facial recognition technology, let us assume, would be used to identify criminals and reduce crime (especially, as we saw above, if integrated with other technologies, such as CCTV camera technology and/or integrated biometric and non-biometric databases, e.g. of passport photos, phone metadata). However, in the hands of politically-driven security agencies in an authoritarian state it may well be used to identify people who are innocent of any crime other than standing up for their human rights. Thus, facial recognition technology, especially taken in conjunction integrated non-biometric (and other biometric) technologies is an instance of dual use technology. Another non-biometric example of dual use technology is encryption – this was designed to protect privacy and confidentiality and, other things being equal, this is a good thing. However, criminals use encryption in ransomware attacks to blackmail organisations to pay them money on pain of not being able to retrieve their data which, in the case of hospitals, may threaten life itself (Miller, 2018 Ch. 7).

In relation to the *avoidable*[18] *outcomes* of the scientific research or technology, we can distinguish: (i) intended outcomes; (ii) unintended but foreseen outcomes; (iii) unforeseen (but foreseeable) outcomes; and (iv) unforeseeable outcomes (Miller, 2018 Ch. 1). An example of an unintended outcome is the spread of radiotoxic material into the environment from a damaged nuclear reactor resulting from a tsunami, as happened in Fukushima, Japan in 2011. However, such accidents are not obviously instances of the dual-use dilemma. For something to be an instance of a dual-use dilemma, both outcomes (the two horns of the dual-use dilemma) need to be (actually or potentially) intended (or at least foreseen or foreseeable) by someone; there needs to be two sets of (actual or potential) *users*. Naturally, an outcome might be unintended and unforeseen (even unforeseeable) by the original researcher or technologist but, nevertheless, intended by the user. Thus, scientists who develop the process of nuclear fission to be used for power generation might not intend or foresee that the same process might be used to build atomic bombs. Again, those who developed facial recognition technology *might* not have intended or foreseen that it might be used by authoritarian governments to assist in the repression of their populations. On the other hand, perhaps this was a foreseeable outcome, if not a foreseen one. Again, the establishment of biometric databases integrated with non-biometric databases (and associated analytics) may well have been driven in many instances by a desire to enhance legitimate law enforcement purposes or to enhance

[18] We are assuming that the relevant outcomes of dual use research are avoidable even if only by refraining from conducting the research. We are further assuming that the scientists in question could have avoided conducting the research. This raises the question of scientists operating in authoritarian states who are coerced into conducting certain research.

health outcomes for the population at large. However, these developments, as already mentioned, have the potential for great harm in the hands of authoritarian states.

Many, if not most, so-called dual use dilemmas are not really dilemmas in the narrow sense of being situations involving two options which are equally morally problematic. In the first place, the dilemmas in question could be tri-lemmas; indeed, there could be four or five or some very large number of options all of which are equally morally problematic. In the second place, the options are not generally *equally* morally problematic. Thus refusing to introduce facial recognition technology or population wide DNA databases might render legitimate law enforcement less effective but introducing either of these might lead to significant violations of citizens' autonomy. Certainly, there are moral considerations for and against each of the options, however it may well be that, all things considered, one of the options is morally preferable to the others and that this is relatively obvious to any rational, morally sensitive person. The point is rather that there are at least some significant moral costs associated with each of the available options. Moreover, there is always the possibility of designing these technologies and the institutional arrangements in which they are embedded in a manner that greatly reducing the potential harms while preserving most of the benefits (van den Hoven et al., 2017). Accountability systems are a way of achieving this in some cases, limiting access to these technologies in other cases (Miller, 2018).

As already noted many, if not most, scientific discoveries and, especially, new technologies, have dual use potential in the trivial sense that they could be used by someone for some malevolent purpose. Indeed, any newly designed object, such as the first baseball bat, has dual use potential in this trivial sense. After all, baseball bats can be used to hit people over the head, as well as for the enjoyment of playing baseball. However, it is implicit in the use of the term "dual use" in play in the academic literature that the potential harm in question is of a very great magnitude and it is caused by a technology (rather than merely a rudimentarily fashioned physical object).

Note that accidents involving science and technology, even accidents on a very large scale, such as the Union Carbide Bhopal chemical disaster and the Chernobyl and Fukushima nuclear disasters, are not *necessarily* dual use in our sense since there is no secondary evil user. More generally, questions of security should be conceptually demarcated from questions of safety.

Nevertheless, such disasters might be dual use if they were predictable. Here two points need to be kept in mind. Firstly, if it is more or less predictable that there will be a *morally culpable large-scale harm-causing* secondary user of the science and technology in question then it may be dual use, notwithstanding that this secondary user did not *intend* to do evil. Perhaps there is gross negligence with respect to safety on the part of a secondary user (who might in fact also be the original researcher) leading to massive loss of life and this was foreseen (or, at least, reasonably foreseeable) by the original researchers. Accordingly, the line between safety and security is in practice blurred; it is blurred at the point at which there is culpable negligence. Culpable negligence is both a safety and a security issue; hence by our

lights dual use issues while primarily matters of security are also to some extent matters of safety. Once again there is an element of stipulation here. However, we are seeking a concept of dual use that does not embrace unforeseeable accidents; surely an unforeseeable accident is not a *use* since it is not an *act* per se but rather an event. The notion of culpability serves our purpose here since, arguably, those who are culpably negligent have committed (in some sense) *acts* of omission. Secondly, the original research which enabled the construction of such industrial plants might be dual use. Thus the process of nuclear fission which has as a by-product highly radioactive fissile material may well be dual use, given the known risk of large-scale harm to humankind posed by such material. Again, health data bases, including genomic data, may be hugely beneficial in part because relied upon by hospitals but if data security is not maintained and, for instance, a ransomware attack renders this data unusable threatening lives, then the harm caused can also be on a very large scale (Miller & Bossomaier, 2021).

Dual use technologies are inherently morally problematic since they are, by definition, technologies that can confer great benefits but also cause (in the wrong hands) great harm. Biometric technologies are no exception. However, the harms potentially caused by biometric technologies are perhaps more insidious that those of some other dual use technologies, e.g. nuclear technology, since biometric technologies do not lend themselves directly to weaponization and, in particular, to being used as WMDs (other than in a figurative sense). This is because although biometric technology enables malevolent actors to cause great harm, it is an essentially epistemic (or knowledge-focussed) technology, e.g. it consists in epistemic action rather than kinetic action (see e.g. Henschke, 2017 Ch. 9; Miller, 2021). Naturally, knowledge enables kinetic action, e.g. identifying someone as a criminal enables his or her arrest. However, identification of an individual via fingerprints, facial images or DNA, even it is a violation of, for instance, their right to privacy, does not necessarily in and of itself cause harm; rather it enables harm to be caused by further kinetic actions.

4.3 Conclusion

The rise of data analytics, smartphones, metadata, social media and artificial intelligence over the past decade has resulted in a broader range of data and identification techniques about individuals to become available, which can by analysed and exploited for a range of purposes. These new forms of data are entwined with, and in some cases facilitated by biometric identification, to constitute a complex contemporary digital identity. Biometric security is likely to play a key role in improving cybersecurity, presently a significant social issue, as well as in relation to online safety, potentially having a role in increasing regulation to address online anonymity. As we have discussed, biometrics – especially when integrated with non-biometric technologies – can be used for beneficial purposes, such as increasing security on devices, identifying criminals or, more generally, greatly increasing the

effectiveness of law enforcement agencies. However, they can also be used for a harmful purpose, such as enabling an authoritarian government to surveil a population. We suggest that law reform arguments in relation to the use of these technologies and associated data can be usefully elucidated through being framed as dual use ethical dilemmas. Appropriate laws should enable biometric identification technologies to be used in ways that benefit society, such as increasing security and efficiency, but regulate and restrict use, so that the potential for privacy violation and other harms are limited as far as possible. Although the use of biometrics can bring great benefits in terms of security, they can also impose great moral costs that raise concerns about liberal democracy in the absence of adequate safeguards, as will be explored further in the final chapter.

References

Australian Criminal Intelligence Commission, Biometric and forensic services. (2021). https://www.acic.gov.au/services/biometric-and-forensic-services

Australia Institute. (2019). *Online harassment and cyberhate costs Australians $3.7b*. https://australiainstitute.org.au/post/online-harassment-and-cyberhate-costs-australians-3-7b/

Australian National University. (2019). *Incident report into the ANU data breach*. https://www.anu.edu.au/news/all-news/data-breach

Australian Parliament. (2021). *Inquiry into family, domestic and sexual violence*. House Standing Committee on Social Policy and Legal Affairs.

Bogle, A. (2020, 27 April). Will the government's coronavirus app COVIDSafe keep your data secure? Here's what the experts say. *Australian Broadcasting Corporation News.*

Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review, 82*, 977–1008.

Burns, W. (2018, 2 February). Is it time to require identity verification for everyone using social media? *Forbes*. https://www.forbes.com/sites/willburns/2018/02/22/is-it-time-to-require-identity-verification-for-everyone-using-social-media/?sh=6bb464528683

De Zwart, M., Humphreys, S., & Van Dissel, B. (2014). Surveillance, big data and democracy: Lessons for Australia from the US and UK. *University of New South Wales Law Journal, 37*, 713–747.

Dencik, L., & Cable, J. (2017). The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication, 11*, 763–765.

Druce, A. (2021, 2 April). It's a long bow': Social media ID push dubbed ineffective, a privacy risk. *Sydney Morning Herald*. https://www.smh.com.au/politics/federal/it-s-a-long-bow-social-media-id-push-dubbed-a-privacy-risk-20210402-p57g7d.html

Federal Bureau of Investigation. (2021). *Next Generation Identification*. https://www.fbi.gov/services/cjis/fingerprintsand-other-biometrics/ngi

Halbfinger, D., Kershner, I., & Bergman, R. (2020, 16 March). To track coronavirus, Israel moves to tap secret trove of cellphone data. *New York Times*. https://www.nytimes.com/2020/03/16/world/middleeast/israel-coronavirus-cellphone-tracking.html

Henschke, A. (2017). *Ethics in an age of surveillance: Virtual identities and personal information*. Cambridge University Press.

Kaye, J., et al. (2015). Dynamic consent: A patient interface for twenty-first century research networks. *European Journal of Human Genetics, 23*, 141–146.

Koper, C., Lum, C., & Willis, J. (2014). Optimizing the use of technology in policing: Results and implications from a multi-site study of the social, organizational, and behavioural aspects of implementing police technologies. *Policing, 8*(2), 212–221.
Meier, O., & Hunger, I. (2014). *Between control and cooperation: Dual-use, technology transfers and the non-proliferation of weapons of mass destruction*. Deutsche Stiftung Friedensforschung.
Miller, S. (2003). Institutions, collective goods and individual rights. *Protosociology, 18*, 184–207.
Miller, S. (2006). Collective moral responsibility: An individualist account. *Midwest Studies in Philosophy, XXX*, 176–193.
Miller, S. (2018). *Dual use science and technology, ethics and weapons of mass*. Springer.
Miller, S. (2020). Freedom of political communication, propaganda and the role of epistemic institutions. In M. Christen, B. Gordjin, & M. Loi (Eds.), *Ethics of cybersecurity*. Springer.
Miller, S. (2021). Rethinking the just intelligence theory of national security intelligence collection and analysis: Principles of discrimination, necessity, proportionality and reciprocity. *Social Epistemology, 35*.
Miller, S., & Bossomaier, T. (2021). *Ethics and cybersecurity*. Oxford University Press.
Miller, S., & Gordon, I. (2014). *Investigative ethics: Ethics for police detectives and criminal investigators*. Blackwell.
Miller, S., & Selgelid, M. (2007). Ethical and philosophical consideration of the dual use dilemma in the biological sciences. *Science and Engineering Ethics, 13*, 523–580.
Miller, S., & Smith, M. (2021). Ethics, public health and technology responses to COVID-19. *Bioethics, 35*.
Miller, S., & Walsh, P. (2016). NSA, Snowden and the ethics and accountability of intelligence gathering. In J. Galliott & J. Reed (Eds.), *Ethics and the future of spying: Technology, intelligence collection and national security* (pp. 193–204). Routledge.
Murphy, J. (2014). *Access to and retention of internet 'metadata'*. Australian Parliamentary Library.
Naeem, S. B. (2020). An exploration of how fake news is taking over social media and putting public health at risk. *Health information and libraries journal, 11*, 1–7.
Nakashima, E., & Albergotti, R. (2021, 14 April). The FBI wanted to unlock the San Bernardino shooter's iPhone. It turned to a little-known Australian firm. *The Washington Post*. https://www.washingtonpost.com/technology/2021/04/14/azimuth-san-bernardino-apple-iphone-fbi/
National Science Advisory Board for Biosecurity (NSABB). (2015). *Framework for conducting risk benefit assessments of gain-of-function research*.
Obar, J., & Wildman, S. (2015). Social media definition and the governance challenge: An introduction to the special issue. *Telecommunications Policy, 39*, 745–750.
Pannett, R., & Birnbaum, M. (2021, 9 June). FBI-controlled anom app ensnares scores of alleged criminals in global police sting. *Washington Post*. https://www.washingtonpost.com/world/2021/06/08/fbi-app-arrests-australia-crime/
Pollack, M. (2019). Taking data. *University of Chicago Law Review, 86*, 77–141.
Pramanik, M., et al. (2017). Big data analytics for security and criminal investigations. *WIREs Data Mining Knowledge Discovery, 7*, 1–19.
Rappert, B., & Selgelid, M. (Eds.). (2013). *On the dual uses of science and ethics: Principles, practices and prospects*. ANU Press.
Ratcliffe, J. H. (2008). Intelligence-led policing. In Wortley, R., & Mazerolle, L. (Eds.), *Chapter 14 of Environmental Criminology and Crime Analysis* (pp. 263–282). Willan Publishing.
Redrup, Y. (2019, 23 July). Experts demand increased transparency in metadata surveillance laws. *Australian Financial Review*.
Sarre, R. (2017). Metadata retention as a means of combatting terrorism and organised crime: A perspective from Australia. *Asian Journal of Criminology, 12*, 167–179.
Selgelid, M. (2016). Gain of function research: Ethical analysis. *Science and Engineering Ethics, 22*, 923–964.
Servick, K. (2020, 21 May). COVID-19 contact tracing apps are coming to a phone near you. How will we know whether they work? *Science*. https://www.sciencemag.org/news/2020/05/countries-around-world-are-rolling-out-contact-tracing-apps-contain-coronavirus-how

Sheng, C., & Zijia, H. (2020, 18 July). Is China's 'health code' here to stay? *The Diplomat*.
Smith, M., & Heath Jeffery, R. (2020). Addressing the challenges of artificial intelligence in medicine. *Internal Medicine Journal, 50*, 1278–1281.
Smith, M., & Urbas, G. (2021). *Technology law*. Cambridge University Press.
Tan, W., et al. (2013). Social-network-sourced big data analytics. *IEEE Internet Computing, 17*, 62–69.
The Guardian. (2020, 16 June). *Norway suspends virus-tracing app due to privacy concerns*. https://www.theguardian.com/world/2020/jun/15/norway-suspends-virus-tracing-app-due-to-privacy-concerns
Tucker, J. (Ed.). (2012). *Innovation, dual use, and security*. MIT Press.
van den Hoven, J., Miller, S., & Pogge, T. (2017). *Designing in ethics*. Cambridge University Press.
Walsh, P., & Miller, S. (2016). Rethinking 'five eyes' security intelligence collection policies and practice post Snowden. *Intelligence & National Security, 31*, 345–368.
Wang, M. (2020, 1 April). China: Fighting COVID-19 with automated tyranny. *The Diplomat*.
Williams, M. (2003). Words, images, enemies: Securitization and international politics. *International Studies Quarterly, 47*, 511–531.
Wong, J. (2019, 18 March). The Cambridge Analytica scandal changed the world: But it didn't change Facebook. *The Guardian*. https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook
World Health Organisation. (2020). *Coronavirus disease situation reports*. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/situation-reports
Zuboff, S. (2019). *The age of surveillance capitalism*. Profile Books.