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 2
Facial Recognition and Privacy Rights

Abstract Biometric facial recognition is one of the most rapidly developing methods of biometric identification, with expanding applications across law enforcement, government and the private sector. Its capacity for integration with other technologies, such as closed circuit television (CCTV) and social media, differentiate it from DNA and fingerprint biometric identification. This chapter commences with a discussion of the technique of facial recognition and applications in identity verification, public surveillance, and the identification of unknown suspects. Its relative advantages and disadvantages, and the development of facial recognition around the world is explored. The discussion then examines how facial recognition databases developed from existing databases, such as driver's licence photographs, can be integrated with CCTV systems, and most recently, with photographs from social media and the internet. The chapter then considers relevant ethical principles, including privacy, autonomy, security and public safety, and the implications for law and regulation in relation to facial recognition.

Keywords Biometric identification · Biometric database · Facial recognition · Closed circuit television (CCTV) · Social media · Privacy · Security

2.1 Facial Recognition

The historical precursor to facial recognition technology is the traditional identification sketch, made on the basis of eyewitness accounts of suspects in criminal investigations (Valentine & Davis, 2015). This was followed by the examination of photographic or CCTV images by an expert, such as an anatomist, when these technologies became available – police and prosecutors are obviously seeking to prove that a specific defendant is depicted in the images and therefore implicated in a crime. This process can involve either quantitative mapping, incorporating the

Note: Some parts of this article were previously published in
Smith, M., & Miller, S. (2021). The ethical application of biometric facial recognition technology. *AI & Society*. https://doi.org/10.1007/s00146-021-01199-9.

M. Smith, S. Miller, *Biometric Identification, Law and Ethics*, SpringerBriefs in Ethics, https://doi.org/10.1007/978-3-030-90256-8_2

comparison of facial feature measurements; or a qualitative examination of the similarities between facial features (Edmond et al., 2009).

Contemporary biometric facial recognition is a digitalised extension of facial mapping, utilising an algorithm to undertake the comparison. In a similar process to that described in fingerprint identification, it is a digital comparison of the arrangement of facial features. The process commences with a digital photograph being taken, and the face scaled and aligned to establish a baseline position. The facial features are then quantified to create a contour map of the position of individual facial features that is converted into a digital template (Ricanek, 2014). In the matching process, pairs of digital templates are compared, and a numerical score derived, representing a probabilistic measure that they are of the same person. System developers establish the threshold of similarity for a match, taking into account a degree of tolerance for false positives and negatives; with scope for a human to make a final determination on a match if necessary (Introna & Nissenbaum, 2010).

The process of verification is undertaken through one-to-one matching: the live comparison of a face with a digital template stored in an identity document, such as a person presenting a passport at border control. In contrast, identification occurs through one-to-many searching: databases of images or CCTV footage are searched in an attempt to establish a match with a photograph of an unknown person. These applications have been respectively described as 'targeted and public' in the case of verification to confirm identity; and 'generalised and invisible' in the case of surveillance in the form of one-to-many searching to identify a suspect (Garvie et al., 2016, p. 2). As will be discussed further shortly, facial recognition can be used to identify people in public places in real time from CCTV footage, or to identify suspects drawing upon the billions of social media images on the internet (Mann & Smith, 2017; Hill, 2020). Facial recognition technology significantly enhances government surveillance capabilities, and in contrast with DNA identification, for example, it can be conducted from a distance without consent.

However, in spite of these advantages over other biometrics, it also has limitations. Facial recognition does not have the same degree of accuracy as fingerprint or DNA identification, and the frequency that facial features occur in the general population is unknown (Smith, et al., 2018). The technique is limited by the quality of images, the similarity of the environment where images were taken, the age of images, the similarity of cameras used, and the size of the cohort of database images for comparison (Introna & Nissenbaum, 2010). Moreover, changes in an individual's face over time, could result in false positive or negative matches. Relevant factors include: aging, cosmetic surgery, make up, weight gain or loss, hair length, glasses, masks and head wear such as scarves (Samuels, 2017). These issues are exacerbated when using facial recognition technology in relation to non-stationary subjects in uncontrolled conditions, such as real-time CCTV footage. In these circumstances, the accuracy of facial recognition can be impacted by magnification, field of view, orientation and light conditions (Grother et al., 2017).

There have been significant applications and legal developments in relation to biometric facial recognition in Australia, the United States and the United Kingdom

over the past 20 years. The technology was integrated into international border control security systems following the 9/11 terrorist attacks on the United States in 2001, and the International Civil Aviation Organisation (ICAO) nominated facial recognition as the global standard for interoperable biometric passports in the early 2000s (Clarke, 2011). Most international airports now have SmartGate technology that automatically scans and compares traveller's faces with biometric identifiers stored within electronic passports (Colley, 2016).

2.1.1 Databases

In contrast with fingerprint or DNA identification databases, governments do not need to obtain facial templates suitable for a facial recognition database specifically for that purpose. Extensive existing repositories (driver licence and passport photographs) have already been created that are suitable for integration with facial recognition technology. Suspect and convicted offender 'mug shot' photograph records are also available, and since 2020, the hundreds of billions of high quality photographs of individuals that have been uploaded to the internet are another potential resource (Hill, 2020). It is clear that facial recognition technology represents a powerful identification tool that has been quickly adopted and integrated with existing law enforcement data systems.

Since 2017, the potential introduction of a national facial biometric matching capability in Australia has been debated, and developments in this jurisdiction provide a useful case study. Legislation has been proposed that would allow a range of federal agencies to share and search facial templates from drivers' licences, passports and other sources. Participating agencies include the Department of Foreign Affairs and Trade, the Department of Home Affairs, the Australian Federal Police, and the Australian Security Intelligence Organisation. Approximately half of the Australian general population hold biometric passports, and the vast majority of the adult population hold drivers licences, meaning that the searching capability of the proposed national database would be approximately 20 million citizens, 80% of the population (Mann & Smith, 2017).

These developments can be traced back to the introduction of biometric passports in the early 2000s. At the state level, incremental legal development has been identified as far back as 2009, when biometric facial recognition compatibility was introduced in New South Wales (NSW) by amending the regulations governing drivers' licences, allowing these images to be searched with biometric systems.[1] In 2015, further regulations were introduced, permitting the release of biometric drivers licence photographs to state police and federal law enforcement and security agencies. Under this change, photographs could be released for biometric matching

[1] The regulations were made pursuant to the *Road Transport* (*Driver Licensing*) *Act 1998* (NSW), which was later repealed by Schedule 1 of the *Road Transport Legislation* (*Repeal and Amendment*) *Act 2013* (NSW).

in relation to the investigation of 'relevant criminal activity', or a 'terrorist act', and this could take place without a warrant or knowledge of the individuals concerned. Because this was effected through a change to regulations, rather than legislation, it occurred without public debate of the capabilities being implemented.

At the federal level in 2015, the government sought to establish a national facial recognition system with the capacity to verify identity through one-to-one matching of documents; and undertake one-to-many searching of databases. In additional to state and territory drivers licence photographs, it also incorporated passport images. In a similar approach to the NSW amendments, the federal government sought to implement this system by changing Commonwealth regulations. The lack of transparency of this approach was criticised, and subsequently legislation was introduced in the national parliament to provide the legal authority for the database (Mann & Smith, 2017).

The legislation authorised the Department of Home Affairs to develop, operate and maintain: an 'interoperability hub' through which participating agencies and organisations can request and transmit biometric facial images and information contained in government identity documents such as driver licenses, but not actually store the images on a federal database. The legislation also proposed that the private sector have limited access to the database to verify the identity of individuals they undertake business with, an aspect that was flagged as creating regulatory complexities and further risks (Mann & Smith, 2017). The Identity-matching Services Bill 2019 and Australian Passports Amendment (Identity-matching Services) Bill 2019 were debated in parliament but not enacted into law, following some critical recommendations of an inquiry by the Parliamentary Joint Committee on Intelligence and Security. The Joint Committee determined that there was insufficient oversight included in the legislation for a system with such significant capabilities, questioning who would be authorised to access the database and under what circumstances, access to the system based on warrants, and a threshold for the seriousness of offences that could be investigated using the system (Petrie, 2019).

2.1.2 CCTV Integration

In the United Kingdom, the Police National Computer (PNC) contains photographs that can be integrated with facial recognition technology, along with other biometrics and intelligence data. It has been reported that the size of this holding is approximately 18 million photographs; however, as with the other jurisdictions discussed, driver's license and passport holdings are a relevant purpose (Hopkins & Morris, 2015). The United Kingdom has been a leader in CCTV integration of facial recognition technology, referred to as Smart CCTV. This provides the capacity to undertake real time surveillance, identification, and tracking of individuals in public places, including the potential identification of individuals in crowds, such as a terrorist suspect at a sports event or a thief in a shopping center. An early example of the use of this technology to receive attention was at the 2017 Champions League

football final in Cardiff, where attendees were compared with a database of persons of interest (Owen, 2017). Facial recognition technology is being used by police in a range of contexts, including in conjunction with cameras fitted to vehicles, body worn cameras, drones and robots: and any other available forms of live video surveillance (Garvie et al., 2016).

In 2019, the High Court of England and Wales considered the issue of biometric facial recognition being used by police in suspect identification (the *Bridges* case).[2] AFR Locate[3] was used by South Wales Police (SWP) to integrate biometric facial recognition technology with live images acquired via a camera attached to a mobile police van, and comparing the images with those listed on a watch list. Mr Bridges claimed that SWP had processed his image using AFR Locate, and that he was not on any watch list, arguing that this unjustifiably breached his rights under Article 8 of the European Convention on Human Rights (ECHR): 'the right to respect for his private and family life, his home and his correspondence'. Further, he argued that the actions of SWP were not 'necessary in a democratic society' for the 'relevant purposes of public safety and crime prevention'.[4]

In 2019, the High Court of England and Wales accepted that the use of AFR Locate interfered with Mr Bridges' privacy rights, but ruled that this was outweighed by the powers of the police to prevent and detect crime. Interestingly, the Court distinguished biometric facial recognition from other police activities that require a warrant because they considered facial recognition technology not to be invasive:

> A warrant is required to allow the police to enter someone's private property since otherwise, the act of entering someone's private property without permission would amount to a trespass. Equally, since the act of taking fingerprints generally requires the cooperation of, or use of force on, the subject and would otherwise amount to an assault, statutory powers were enacted to enable the police to take fingerprints. Both involve physically intrusive acts. By contrast, the use of AFR Locate to obtain biometric information is very different. No physical entry, contact or force is necessary when using AFR Locate to obtain biometric data. It simply involves taking a photograph of someone's face and the use of algorithms to attempt to match it with photographic images of faces on a watchlist. The method is no more intrusive than the use of CCTV in the streets.[5]

---

[2] *R* (*on the application of Edward Bridges*) *v The Chief Constable of South Wales* [2019] EWHC 2341.

[3] AFR (Automated Facial Recognition).

[4] European Convention on Human Rights Article 8 – Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[5] [2019] EWHC 2341, 75.

A further issue raised by Mr Bridges was that the AFR Locate technology was new and not regulated by any specific legislation. However, the Court found that this did not preclude its use either:

> In our view, there is a clear and sufficient legal framework governing whether, when and how AFR Locate may be used. What is important is to focus on the substance of the actions that use of AFR Locate entails, not simply that it involves a first-time deployment by SWP of an emerging technology. The fact that a technology is new does not mean that it is outside the scope of existing regulation, or that it is always necessary to create a bespoke legal framework for it.[6]

This decision was appealed to the England and Wales Court of Appeal in 2020,[7] which reversed the 2019 decision, finding that the live automated facial recognition technology used by the South Wales Police Force was unlawful under Article 8 of the ECHR. The Court stated:

> The fundamental deficiencies, as we see it, in the legal framework currently in place relate to two areas of concern. The first is what was called the "who question" at the hearing before us. The second is the "where question". In relation to both of those questions too much discretion is currently left to individual police officers. It is not clear who can be placed on the watchlist nor is it clear that there are any criteria for determining where AFR can be deployed.[8]

A longstanding regulatory development in the United Kingdom is the independent statutory commissioner, established to oversee and respond to concerns relating to consent, retention and use of biometric information by law enforcement agencies in the United Kingdom. The Commissioner for the Retention and Use of Biometric Material[9] seeks to improve the regulation of biometric information and provide a degree of protection from disproportionate law enforcement action.[10] While the Commissioner's powers only currently extend to DNA or fingerprints (OBC, 2020); the House of Commons Science and Technology Committee has recommended that these statutory responsibilities 'be extended to cover, at a minimum, the police use and retention of facial images' (HCSTC, 2015), which may be an impending development after the decision in *Bridges*.

---

[6] [2019] EWHC 2341, 84.

[7] *R* (*on the application of Bridges*) *v Chief Constable of South Wales Police* (2020] EWCA Civ 1058.

[8] Ibid, 91.

[9] The UK Biometrics Commissioner was established under the *Protection of Freedoms Act 2012* (UK) in response to the judgement in the *S and Marper v United Kingdom* [2008] ECHR 1581 case in the European Court of Human Rights in 2008.

[10] *Protection of Freedoms Act 2012* (UK) c 9, s 20.

2.1.3 Social Media Integration

The use of facial recognition technology by social media companies headquartered in the United States, followed the development of government databases since 2000, which will initially be briefly considered. The federal facial recognition database is known as the Next Generation Identification (NGI) system. Operated by the Federal Bureau of Investigation, it integrates facial templates with biometrics and other forms of intelligence and has the capacity to search state driver's license databases and other vast repositories. The FBI's facial-recognition capability facilitates 'access to local, state and federal databases containing more than 641 million face photos' (Harwell, 2019). These databases include the US Visitor and Immigrant Status Indicator Technology (US-VISIT) program which collects biometrics from all non-citizens entering the US. Other agencies that may have access to facial recognition searching in the United States include Customs and Border Protection, Coast Guard, Citizenship and Immigration Services, the Department of State, Department of Defence, and Department of Justice, as well as the law enforcement and intelligence communities. On a case-by-case basis, the United States government provides access to facial image repositories for partner countries such as Australia, Canada, New Zealand, and the United Kingdom (USDHS, 2015). In recent years, access to state drivers license databases for facial recognition searching without legislative backing at the state or federal level, or consent of the individuals concerned, has been controversial and debated in congress – further law reform is likely (Harwell, 2019).

The private sector in the United States, in collaboration with law enforcement agencies, have been pioneering another significant application of facial recognition – the analysis of internet-based images from social media sites such as Facebook, Twitter, Instagram, LinkedIn, and Google. There has been a massive expansion in the number of images available on the Internet in recent years: in 2012, Facebook alone held over 100 billion photos in its database, by 2020 that number more than doubled to 250 billion (Hill, 2020).

Facebook uses facial recognition technology to 'tag' photographs with users' names, linking images to individuals' pages and also allowing individuals to be tagged irrespective of whether they have a Facebook page. The Hamburg Commissioner of Data Protection launched a legal challenge to Facebook's facial recognition tagging feature under German data protection and privacy laws; and in 2012, the Irish Data Protection Commissioner audited Facebook's use of face recognition that led to Facebook disabling this feature in the Europe, and deleting stored biometric information previously collected (Mann & Smith, 2017). In 2018, it returned as an opt-in feature in Europe, but remains an opt-out feature in other regions of the world (Kelion, 2018).

In 2020, it became public that police in the United States were using a facial recognition algorithm, developed by the technology company Clearview AI, to search images on the internet in an attempt to identify suspects in investigations (Hill, 2020). It was also reported that police in other countries around the world,

such as Australia, were also using Clearview AI's algorithm (Bogle, 2020). Compared with national databases of passport and drivers' licence images, or scanning CCTV footage for suspects; the Clearview AI development, with a capacity to search billions of facial images on the internet in minutes, represents a massive advancement. Significantly, it was also reported that Clearview AI was not only providing facial recognition software to law enforcement agencies, but also private companies, such as Walmart, AT&T, the NBA, Bank of America and Best Buy, for private security purposes.[11]

Legal action against Clearview AI has since commenced. Immediately after the use of the company's services was publicised, the State of New Jersey and social media companies, including Twitter and Facebook, sent cease-and-desist letters asserting that the company had unlawfully obtained users' images (BBC, 2020). A number of class actions were launched. One of these, commenced against Clearview AI by the law firm Haeggquist & Eck, LLP, alleged that Clearview AI violated the provisions of a number of statutes, including the *California Consumer Privacy Act of 2018* (CCPA), raising several issues on behalf of the plaintiffs:

- The individuals did not consent to the use or redistribution of photographs, biometric information and identifiers;
- Clearview AI 'scraped' the images from internet-based websites, in violation of several of the websites' terms of use;
- Clearview AI applied facial recognition software in violation of the CCPA and BIPA;
- Clearview AI sold access to photographs, biometric information and identifiers to third-party entities for commercial gain without consent; and
- Damages were suffered in terms of the diminution in value of individuals' biometric information, and identifiers and placed them at risk of privacy violation.[12]

West (2021) describes the role of social media posts in the investigation of the violence that occurred at the United States Capitol in January 2021, following the outcome of the presidential election. Many rioters posted incriminating images of themselves in and around the Capitol Building, including committing crimes such as trespass and vandalism. The Federal Bureau of Investigation was able to quickly identify many of those responsible, in some cases within hours of the offences being committed, with very strong evidence to provide to prosecutors and obtain a conviction. The role of social media in both enabling the event and in holding those responsible accountable is interesting to observe.

These recent developments add further complexity to the legal and ethical issues associated with biometric facial recognition– the reported use of the technology by

[11] Statement of Claim, *State of Vermont v Clearview AI, Vermont Superior Court*, 10 March 2020, 8.

[12] Haeggquist & Eck, LLP, *Sean Burke and James Pomerene, Individually and on Behalf of All Others Similarly Situated, Plaintiffs v. Clearview AI, Inc., a Delaware Corporation*; *Hoan Ton-That, an Individual*; *Richard Schwartz, an Individual*; *and Does 1 through 10, inclusive, Defendants*, United States District Court Southern District of California. Class Action Complaint Demand for Jury Trial. Case Number: 20CV0370 BAS MSB, 5–8.

private sector companies such as banks and retailers is more concerning than use by law enforcement. While legal constraints associated with Clearview AI's use of images held by social media companies may ultimately threaten its feasibility and ability to provide its services to the private sector; this is less likely to be an issue for a law enforcement agency, and further regulation and guidance through legislative reform is needed.

2.2 Ethical Principles

The expanding use of biometric facial recognition raises a number of pressing ethical concerns for liberal democracies. The concerns relate especially to the potential conflicts between security, on the one hand, and individual privacy and autonomy, and democratic accountability, on the other. Security and community safety are fundamental values in liberal democracies, as in other polities, including many authoritarian ones. However, liberal democracies are also committed to individual privacy and autonomy, democracy, and therefore, democratic accountability. Accordingly, the latter fundamental ethical principles must continue to be valued in ~~a~~ liberal democracies such as Australia, the United Kingdom and the United States, notwithstanding the benefits to security and community safety that biometric facial recognition can provide (Miller & Bossomaier, 2021). While debates will continue between proponents of security, on the one hand, and defenders of privacy, on the other, there is often a lack of clarity in relation to the values or principles allegedly in conflict.

2.2.1 Privacy

The notion of privacy has proven difficult to adequately explicate (Benn, 1988; Miller, 1997; Etzioni, 1999; Miller & Weckert, 2000; Nagel, 2002; Kleinig et al., 2011). Nevertheless, there are a number of general points that can be made (Benn, 1988; Miller, 1997; Nagel, 2002; Macnish, 2017; Henschke, 2017). First, privacy is a right that people have in relation to other persons, the state and organisations with respect to: (a) the possession of information (including facial images) about themselves by other persons and by organisations, e.g. personal information and images stored in biometric databases, or; (b) the observation/perceiving of themselves – including of their movements, relationships and so on – by other persons, e.g. via surveillance systems including tracking systems that rely on biometric facial images. Biometric facial recognition is obviously implicated in both informational and observational concerns.

Second, the right to privacy is closely related to the more fundamental moral value of autonomy (Benn, 1988; Miller, 1997; Nagel, 2002). Roughly speaking, the notion of privacy delimits an informational and observational 'space' i.e. the private sphere. However, the right to autonomy consists of a right to decide what to think

and do and, of relevance here, the right to control the private sphere and, therefore, to decide *who to exclude and who not to exclude* from it. So the right to privacy consists of the right to exclude organisations and other individuals (the right to autonomy) both from personal information and facial images, and from observation and monitoring (the private sphere).

As noted in Chap. 1, the moral right to control some element of the private sphere does not necessarily depend on the difficulty attaching to exercising that right. A person has a moral right that others not trespass on his land, irrespective of whether his land is fenced or he has the means to exclude them. Again, a person has a moral right not to be photographed in her shower, irrespective of whether or not a long range camera is able to take photo of her in the shower in her home from outside her property. The 2019 High Court of England and Wales decision in *Bridges* did not invoke this morally (but perhaps not legally) relevant conceptual distinction. In the 2020 Court of Appeal decision, the Court raised what they termed the 'where question' finding that there appeared to be too much discretion left to individual police officers with respect to where they could deploy the technology, in addition to the question of who it could lawfully be deployed against, in light of Article 8 of the ECHR.

By contrast with the degree of difficulty attaching to exercising one's right, the moral right to control some element of the privacy sphere can depend on the moral weight of that element and, of relevance to facial technology, it's centrality to a person's personal identity (Nagel, 2002 Ch. 1; Henschke, 2017). Evidently, one's face is constitutive of one's personal identity; hence one has a moral right to control images of one's face. Conversely, it might be argued that one's face is necessarily present to others and, therefore, one does not, because one cannot, have a right to control images of it. Certainly, one's face is a central tool of interpersonal expression and communication. However, it does not follow from this that one does not have a right to control images of it. Firstly, we need to distinguish one's face from images of it. Logically, one could have a right to control images of one's face even if one had limited control over who saw one's face in the flesh (so to speak). Secondly, one can in fact exercise considerable control over which interpersonal contexts one participates in and, therefore, who sees one's face. Moreover, one can also exercise control over how one presents one's self in the company of others, e.g. one can choose to conceal or feign emotions by controlling one's facial expressions. Secondly, speaking generally, in these interpersonal context the faces of all those who participate are visible to the others. It is not simply a case of one party doing the looking without being themselves looked at, as is the case with the uncontrolled (by one's-self) dissemination of one's facial image.

Naturally, the right to privacy is not absolute; it can be overridden. Moreover, its precise boundaries are unclear; a person does not have a right not to be observed in a public space but, arguably, has a right not to be photographed in a public space (let alone have an image of their face widely circulated on the internet), albeit this right not to be photographed and have one's image circulated can be overridden under certain circumstances (Miller & Gordon, 2014 Ch. 10; Miller & Blackler, 2016 Ch. 4; Kleinig et al., 2011). For instance, this right might be overridden if the public

space in question is under surveillance by CCTV in order to detect and deter crime, and if the resulting images are only made available to police – and then only for the purpose of identifying persons who have committed a crime in that area. What of persons who are present in the public space in question and recorded on CCTV, but who have committed a serious crime, such as terrorism, elsewhere, or at least are suspected of having committed a serious crime[13] elsewhere and are, therefore, on a watch-list? Presumably, it is morally acceptable to utilise CCTV footage to identify these persons as well. If so, then it seems morally acceptable to utilize biometric facial recognition technology to match images of persons recorded on CCTV with those of persons on a watch-list of those who have committed, for instance, terrorist actions, or are suspected of having done so, as the SWP were arguably seeking to do in the *Bridges* case.

Third, a degree of privacy is necessary simply in order for people to pursue their personal projects, whatever those projects might be (Benn, 1988). For one thing, reflection is necessary for planning, and reflection requires a degree of freedom from the distracting intrusions, including intrusive surveillance, of others. For another, knowledge of someone else's plans can lead to those plans being thwarted (e.g. if one's political rivals can track one's movements and interactions then they can come to know one's plans in advance of their implementation), or otherwise compromised, (e.g. if who citizens vote for is not protected by a secret ballot, including a prohibition on cameras in private voting booths, then democracy can be compromised).

We have so far considered the rights of a *single* individual; however, it is important to consider the implications of the infringement, indeed violation, of the privacy and autonomy rights of the whole citizenry by the state (and/or other powerful institutional actors, such as corporations). Such violations on a large scale can lead to a power imbalance between the state and the citizenry and, thereby, undermine liberal democracy itself (Miller & Walsh, 2016). The surveillance system imposed on the Uighurs in China, incorporating biometric facial recognition technology, graphically illustrates the risks attached to large scale violations of privacy and related autonomy rights.

Accordingly, while it is morally acceptable to collect biometric facial images for necessary circumscribed purposes, such as passports for border control purposes and drivers' licences for safety purposes, it is not acceptable to collect them to establish vast surveillance states as China has done, and exploit them to discriminate on the basis of ethnicity. However, images in passports and driving licences are, and arguably ought to be, available for *wider* law enforcement purposes, e.g. to assist in tracking the movements of persons suspected of serious crimes unrelated to border control or safety on the roads. The issue that now arises is the determination of the point on the spectrum at which privacy and security considerations are appropriately balanced.

[13] We will define a serious crime as an offence punishable by imprisonment for a term of 3 or more years.

Privacy can reasonably be overridden by security considerations under some circumstances, such as when lives are at risk. After all, the right to life is, in general, a weightier moral right than the right to privacy (Miller & Blackler, 2016 Ch. 4; Miller & Gordon, 2014 Ch. 10; Miller & Walsh, 2016). Thus, utilising facial recognition technology to investigate a serious crime such as a murder or track down a suspected terrorist, if conducted under warrant, is surely ethically justified. On the other hand, intrusive surveillance of a suspected petty thief might not be justified, even assuming it is very effective. Here key principles that need to be invoked are necessity and proportionality (Miller, 2021; Henschke, 2017; Macnish, 2017). Is it necessary to use facial recognition technology or would a less invasive means suffice? And, even if it is necessary, is it proportionate? Evidently, widespread use of facial recognition technology in conjunction with facial recognition technology would be a disproportionate response to a few instances of petty crime. Moreover, given the importance of, so to speak, the aggregate privacy/autonomy of the citizenry, threats to life on a small scale might not be of sufficient weight to justify substantial infringements of privacy/autonomy, e.g. a low level terrorist threat might not justify citizen-wide biometric facial recognition database. Again, the principles of necessity and proportionality are relevant, albeit this time at the macro society-wide level (Miller, 2021). Further, regulation, and associated accountability mechanisms need to be in place to ensure that, for instance, a database of biometric facial images created for a legitimate purpose, e.g. a repository of passport photos, can be accessed by border security and law enforcement officers to enable them to prevent and detect serious crimes, such as murder, but not used to identify protesters at a political rally.

We have argued that privacy rights, including in respect of biometric facial images, are important, in part because of their close relation to autonomy, and although they can be overridden under some circumstances, notably by law enforcement investigations of serious crimes (and given it is effective, necessary and proportionate), there is obviously a point where infringements of privacy rights is excessive and unwarranted. This is obviously the case in relation to privacy rights infringed, indeed violated, simply to generate profits, as in the case of a business model that provides ‘free’ services in return for personal data without *strong* consent (see Chap. 1), e.g. Facebook’s business model. A national biometric facial recognition database for use in relation to serious crimes, and subject to appropriate accountability mechanisms may be acceptable, but utilising billions of images from social media accounts (e.g. in the way that Clearview AI’s technology does) to detect and deter minor offences, let alone establishing a surveillance state (e.g. to the extent that has been achieved in China), is clearly unacceptable. Let us now turn directly to security.

2.2.2 *Security and Public Safety*

Security can refer to, for example, national security (such as harm to public from a terrorist attack), community security (such as in the face of disruptions to law and order) and organisational security (such as breaches of confidentiality and other forms of misconduct and criminality). At other times it is used to refer to personal physical security. Physical security in this sense is security in the face of threats to one's life, freedom or personal property – the latter being goods to which one has a human right. Violations or breaches of physical security obviously include assault and murder (Miller & Gordon, 2014; Miller & Blackler, 2016; Miller & Bossomaier, 2021). Biometric facial recognition systems could assist in multiple ways to enhance security in each of these senses. Thus a biometric facial recognition system could help to prevent fraud by better establishing identity (e.g. identify people using falsified drivers licences) and facial recognition data would be likely to help to investigate serious crimes against persons (e.g. identifying unknown suspects via CCTV footage). However, as mentioned above, its use in relation to less serious crimes, e.g. crimes, such as shoplifting, that are punishable by a prison term of, say, less than three years, evidently would not comply with the principle of proportionality in particular.

Arguably, security should be distinguished from safety, although the two concepts are related and the distinction somewhat blurred (Miller, 2018 Ch. 5 Sec. 5.2). We tend to speak of safety in the context of wildfires, floods, pandemics and the like, in which the harm to be avoided is not intended harm. By contrast, the term 'security' typically implies that the threatened harm is intended. At any rate, it is useful to at least maintain a distinction between intended and unintended harms and, in relation to unintended harms, between foreseen, unforeseen and unforeseeable harms. For instance, someone who is unknowingly carrying the COVID-19 virus because they are asymptomatic, is a danger to others but, nevertheless, might not be culpable (if, for instance, they had taken reasonable measures to avoid being infected, had an intention to test for infection if symptoms were to arise and, if infected, would take all possible measures not to infect others). While biometric facial recognition systems can make an important contribution to security, their utility in relation to safety is less obvious, albeit they could assist in relation to finding missing persons or ensuring unauthorised persons do not unintentionally access dangerous sites (Smith & Miller, 2021).

We have described the expanding use of biometric facial recognition for security and public safety purposes and elaborated on current applications and legal developments in Australia, the United States and the United Kingdom. In light of these applications and developments, we have discussed various ethical principles and concepts, notably privacy and security. We now need to consolidate and specify a number of the more salient ethical problems and principles that arise from the expanding use of biometric facial recognition for security purposes, especially in the context of interlinkage with non-biometric databases, data analytics and artificial intelligence.

First, privacy in relation to personal data, such as facial images, consists in large part in the right to control the access to, and use of, that data. Moreover, given that one's face is a constitutive feature of one's personal identity one has a moral right to exercise control of one's facial images, albeit this moral right is not absolute. Accordingly, this moral right can be overridden by other rights, such as the right to security. However, security consists in large part in individual rights, notably the right to life, as well as to institutional goods, such as law and order. Biometric facial recognition technology gives rise to security concerns, such as the possibility of identity theft by a sophisticated malevolent actor, even as they resolve old privacy and confidentiality concerns, such as by reducing unauthorised access to private information and thereby strengthening privacy protection. In short, the problems in this area cannot be framed in terms of a simple weighing of, let alone trade-off between, individual privacy rights versus the community's interest in security.

Second, the establishment of comprehensive, integrated biometric facial recognition databases and systems by governments (and now the private sector), and the utilisation of this data to identify and track citizens, (e.g. via live CCTV feeds) has the potential to create a power imbalance between governments and citizens, and risks undermining important principles taken to be constitutive of the liberal democratic state, such as privacy.

Third, the security contexts in which their use is to be permitted might become both very wide and continuing, e.g. the counter-terrorism ('emergency') security context becomes the 'war' (without end) against terrorism; which becomes the war (without end) against serious crime; which becomes the 'war' (without end) against crime in general (Miller & Gordon, 2014).

Fourth, the expanding use of biometric facial recognition databases and systems has to be clearly and demonstrably justified in terms of efficiency and effectiveness in the service of *specific* security and/or safety purpose, rather than by general appeals to community security or safety. Relatedly, data, including surveillance data, originally and justifiably gathered for one purpose, e.g. taxation or combating a pandemic, is interlinked with data gathered for another purpose, e.g. crime prevention, without appropriate justification (Miller & Gordon, 2014 Ch. 10; Miller & Blackler, 2016 Ch. 4). The way metadata use has expanded from initially being used by only a few agencies to now being used quite widely by governments in many western countries, is an example of function creep and illustrates the potential problems that might arise with the introduction of biometric facial recognition systems (Mann & Smith, 2017).

Fifth, various general principles taken to be constitutive of liberal democracy are gradually undermined, such as the principle that an individual has a right to freedom from criminal investigation or unreasonable monitoring, absent prior evidence of violation by that individual of its laws. In a liberal democratic state, it is generally accepted that the state has no right to seek evidence of wrongdoing on the part of a particular citizen or to engage in selective monitoring of that citizen, if the actions of the citizen in question have not otherwise reasonably raised suspicion of unlawful behaviour and if the citizen has not had a pattern of unlawful past behaviour that justify monitoring. Moreover, in a liberal democratic state, it is also generally

accepted that there is a presumption against the state monitoring the citizenry. This presumption can be overridden for specific purposes but only if the monitoring in question is not disproportionate, is necessary or otherwise adequately justified and kept to a minimum, and is subject to appropriate accountability mechanisms (Miller, 2021). Arguably, the use of CCTV cameras in crime hot-spots could meet these criteria if certain conditions were met, e.g. police access to footage was granted only if a crime was committed or if the movements of a person reasonably suspected of a crime needed to be tracked. However, these various principles are potentially undermined by certain kinds of offender profiling and, specifically, ones in which there is no specific (actual or reasonably suspected) past, imminent or planned crime being investigated (Miller & Gordon, 2014 Ch. 10; Miller & Blackler, 2016 Ch. 4). Biometric facial recognition could be used to facilitate, for instance, a process of offender profiling, risk assessment and subsequent monitoring of people who as a result of fitting these profiles are considered at risk of committing crimes, notwithstanding that the only offences that the individuals in question had committed was to fit these profiles.

Finally, in so far as the use of facial recognition and other biometric identification systems can be justified for specific security (and safety) purposes and, therefore, privacy and other concerns mitigated, it is, nevertheless, imperative that their use be subject to accountability mechanisms to guard against misuse. Citizens should be well informed about biometric facial recognition systems and should have consented to the use of these systems for the specific, justified purposes in question. Their use should be publicly debated, backed by legislation, and their operation subject to judicial review.

2.3 Conclusion

Biometric facial recognition is rapidly becoming very widely used by government and the private sector. It can integrate existing photographs, such as those stored in driver's license registries or posted on the internet and combine with CCTV networks to identify individuals in public spaces. Recent examples, such as the debate about Clearview AI, demonstrate the high value law enforcement agencies place on this form of data, and the concern held by the community in relation to its use for this purpose. We have described the notion of privacy and its relation to autonomy. We have also described the relationship between facial images and personal identity. Biometric facial recognition (in both informational and observational aspects) has the potential to unacceptably compromise privacy, autonomy and personal identity rights; indeed, as mentioned above, it is already being used to do so in Xinjiang in China. Applying the principles of necessity and proportionality, it may be acceptable to use facial recognition in association with CCTV to identify an individual, for example who has, or is suspected of having committed, a serious crime or act of terrorism. However, the use of facial recognition technology in conjunction with CCTV to monitor ordinary citizens (as opposed to monitor a restricted area or to

create footage which is only accessed if, for instance, a crime is committed) is not acceptable and should be restricted by legislative protections to prevent this being done on a wide scale and for political purposes, as in China. Moreover, access to CCTV footage should be restricted by law, both in terms of those who are granted access and the purposes for which they are granted access, and access should be subjected to stringent accountability mechanism. Footage should only be destroyed after a reasonable time period other than in exceptional circumstances (e.g. if used in the investigation of a serious crime, and associated court proceedings). Further, the creation of national, and especially universal, facial recognition databases for law enforcement and security purposes from existing repositories of facial images, such as passport or drivers licence databases, is an example of morally unacceptable function creep. More generally, the creation of facial recognition databases needs to be justified in terms of specific, defined, morally acceptable purposes and not, therefore, merely by general appeals to vague notions of community safety, national security, and the like. Moreover, facial recognition databases should not be established without public debate, the consent of the citizenry and supporting legislation and accountability mechanisms.

References

Benn, S. I. (1988). *Theory of Freedom*. Cambridge University Press.

British Broadcasting Corporation (BBC). (2020, January 23). *Twitter demands AI company stops collecting faces*. https://www.bbc.com/news/technology-51220654

Bogle, A. (2020, April 14). Australian federal police officers trialled controversial facial recognition tool Clearview AI. *Australian Broadcasting Corporation News*. https://www.abc.net.au/news/science/2020-04-14/clearview-ai-facial-recognition-tech-australian-federal-police/12146894

Clarke, S. (2011). Balancing privacy and security in the Australian passport system. *Deakin Law Review, 16*(2), 325–360.

Colley, A. (2016, October 21). Govt wants to remove passports from border processing. *IT News*. https://www.itnews.com.au/news/govt-wants-to-remove-passports-from-border-processing-439785

Edmond, G., Biber, K., Kemp, R., & Porter, G. (2009). Law's looking glass: Expert identification evidence derived from photographic and video images. *Current Issues in Criminal Justice, 20*(3), 337–377.

Etzioni, A. (1999). *Limits of privacy*. Basic Books.

Garvie, C., Bedoya, A., & Frankle, J. (2016). *The perpetual line-up*: *Unregulated police face recognition in America*. Georgetown Law Centre on Privacy and Technology Report. https://www.perpetuallineup.org/

Grother, P., Quinn, G., & Ngan, M. (2017). *Face in video evaluation* (*FIVE*): *Face recognition of non-cooperative subjects*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8173.pdf

Harwell, D. (2019, July 8). FBI, ICE find state Driver's license photos are a gold mine for facial-recognition searches. *Washington Post*. https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/

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

Hill, K. (2020, January 18). The secretive company that might end privacy as we know it. *New York Times.* https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

Hopkins, N., & Morris, J. (2015, February 3). Innocent people on police photos database. *British Broadcasting Corporation News*. http://www.bbc.com/news/uk-31105678

House of Commons Science and Technology Committee (HCSTC). (2015). *Current and future uses of biometric data and technologies*. United Kingdom Parliament.

Introna, L., & Nissenbaum, H. (2010). Facial recognition technology: A survey of policy and implementation issues. *Lancaster University Working Paper*. http://www.research.lancs.ac.uk/portal/en/publications/facial-recognition-technology-a-survey-of-policy-and-implementation-issues(43367675-c8b9-4644-90f2-86815cc8ea15).html

Kleinig, J., Mameli, P., Miller, S., Salane, D., & Schwartz, A. (2011). *Security and privacy*. ANU Press.

Kelion, L. (2018, April 18). Facebook seeks facial recognition consent in EU and Canada. *British Broadcasting News*. https://www.bbc.com/news/technology-43797128

Macnish, K. (2017). *Surveillance ethics: An introduction*. Routledge.

Mann, M., & Smith, S. (2017). Automated facial recognition technology: Recent developments and approaches to oversight. *UNSW Law Journal, 40*, 121–145.

Miller, S. (1997). Privacy and the internet. *Australian Computer Journal, 29*(1), 12–16.

Miller, S. (2018). *Dual use science and technology, Ethics and weapons of mass destruction*. 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*, 211–231.

Miller, S., & Blackler, J. (2016). *Ethical Issues in Policing*. Routledge.

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., & 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.

Miller, S., & Weckert, J. (2000). Privacy, the workplace and the internet. *Journal of Business Ethics, 14*(2), 255–265.

Nagel, T. (2002). *Concealment and exposure, and other essays*. Oxford University Press.

Office of the Biometrics Commissioner (OBC). (2020). *About.* https://www.gov.uk/government/organisations/biometrics-commissioner/about

Owen, G. (2017, April 26). British cops will scan every fan's face at the champions league final. *Motherboard*. https://motherboard.vice.com/en_us/article/british-cops-will-scan-every-fans-face-at-the-champions-league-final

Petrie, C. (2019, August 26). *Bills digest No. 21 identity-matching Services Bill 2019 and Australian Passports Amendment* (*Identity-matching Services*) *Bill 2019*. Australian Parliamentary Library.

Ricanek, K. (2014, September). Beyond recognition: The promise of biometric analytics. *IEEE Computer Society, 47*, 87–89.

Samuels, G. (2017, January 5). Anti-surveillance clothing unveiled to combat facial recognition technology. *The Independent*. http://www.independent.co.uk/news/science/anti-surveillance-clothing-facial-recognition-technology-hyperface-adam-harvey-berlin-facebook-apple-a7511631.html

Smith, M., Mann, M., & Urbas, G. (2018). *Biometrics, Crime and Security*. Routledge.

Smith, M., & Miller, S. (2021). The ethical application of biometric facial recognition technology. *AI & Society*. https://doi.org/10.1007/s00146-021-01199-9

United States Department of Homeland Security. (2015). *DHS/NPPD/privacy impact assessment*: *Automated biometric identification system* (*IDENT*). https://www.dhs.gov/publication/dhsnppdpia-002-automated-biometric-identification-system-ident

Valentine, T., & Davis, J. (2015). *Forensic facial identification: Theory and practice of identification from eyewitnesses and CCTV*. Blackwell.

West, D. (2021). *Digital fingerprints are identifying Capitol rioters*. The Brookings Institution. https://www.brookings.edu/blog/techtank/2021/01/19/digital-fingerprints-are-identifying-capitol-rioters/