SpringerBriefs in Ethics

Springer Briefs in Ethics envisions a series of short publications in areas such as business ethics, bioethics, science and engineering ethics, food and agricultural ethics, environmental ethics, human rights and the like. The intention is to present concise summaries of cutting-edge research and practical applications across a wide spectrum.

Springer Briefs in Ethics are seen as complementing monographs and journal articles with compact volumes of 50 to 125 pages, covering a wide range of content from professional to academic. Typical topics might include:

- Timely reports on state-of-the art analytical techniques
- A bridge between new research results, as published in journal articles, and a contextual literature review
- A snapshot of a hot or emerging topic
- In-depth case studies or clinical examples
- Presentations of core concepts that students must understand in order to make independent contributions

More information about this series at https://link.springer.com/bookseries/10184

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 1
The Rise of Biometric Identification: Fingerprints and Applied Ethics

Abstract In the late nineteenth century, it became understood that the patterns on the skin of the fingers were unique and could be used for identification purposes, leading to the development of biometric identification (Smith M, Mann M, Urbas G. Biometrics, crime and security. Routledge, 2018). The ease with which fingerprints can be accessed and recorded, and the ease with which they transfer to surfaces and objects, made them ideal for law enforcement purposes. Today, in digital form, fingerprints and other biometric identification techniques, notably DNA profiles and facial recognition technology, are a widely used means of identification across a range of applications, from accessing personal devices, to banking, border security and law enforcement. However, these uses have raised a raft of ethical or moral (we use these terms interchangeably) concerns, some of the more important of which we discuss in this work.

In the first chapter, we discuss general aspects of biometric identification, before focusing on fingerprint identification, including its reliability as form of evidence. Secondly, we provide an overview of applied ethics; and outline a key theoretical notion, relevant to many of the issues discussed throughout the later chapters: collective responsibility. Finally, we analyse the ethical risks and benefits associated with the technique of fingerprint identification.

Keywords Biometric identification · Fingerprint identification · Criminal investigation · Applied ethics · Collective responsibility · Joint action

1.1 Overview of Biometric Identification

Biometrics refers to the measurement of physical aspects of the human body. This can include patterns of the skin or blood vessel networks under the skin; patterns in the genetic code; facial appearance, such as the distance between features such as the eyes, nose or mouth; and behavioural traits, such as gait (Smith et al., 2018). For identification purposes, in addition to being a physical feature capable of being measured, biometrics must be unique between individual humans, able to be efficiently verified, and unchanging over time. They must also be capable of being

M. Smith, S. Miller, *Biometric Identification, Law and Ethics*, SpringerBriefs in Ethics, https://doi.org/10.1007/978-3-030-90256-8_1

digitalised through an algorithm and converted to a format that can be integrated with automated database storage and searching.

Biometric identification can be contrasted with other methods of identification, such as keys, identification cards and passwords. The obvious distinction being that a biometric is a reference to part of the individual themselves, rather than an object carried on the person, or password held in their mind. Biometric identification has been described as: rather than being something that an individual *knows* or *has*, it is something that they *are* (Hopkins, 1999).

The first known application of a form of biometric identification took place in Ancient Egypt, for the purpose of ensuring that food provided by the state was shared equitably among those legitimately eligible to receive it. A system was developed to record distinctive physical and behavioural characteristics of workers, along with their name, age and place of residence, to ensure individuals did not obtain more than their allocated allowance. A significant development occurred in the mid-nineteenth century, when Czech scientist Jan Evangelista Purkinje (1787–1869) established that fingerprints were unique (Ashbourn, 2000). The classification system for fingerprints was developed by Sir Francis Galton (1882–1911) and Sir Edward Henry (1850–1931). The Henry classification system provided a method to classify fingerprints and exclude potential match candidates, establishing fingerprinting as a basis for individual identification and the foundation of fingerprint databases. This was quickly adopted by law enforcement agencies, led by Scotland Yard, and databases were later developed in collaboration with the private sector, throughout the twentieth century (Allen et al., 2005).

Fingerprint identification became the central identification tool in criminal investigation until the mid-1980s, when it was overshadowed by the arrival of DNA profiling; however, it remains relevant today (Smith, 2016). Over the past decade, facial recognition technology has been an area of advancement within the field of biometrics, alongside a range of new DNA profiling techniques. The past decade has also seen the expansion of biometrics in society, from personal devices such as laptops and smartphones, to building access and banking services, it is rapidly replacing traditional methods of access and identity verification such as keys and personal identification numbers.

Biometrics can be used for one-to-many searching, where an unknown individual's biometric profile is compared with a database of profiles to identify them, such as in a criminal investigation context. It can also be used for one-to-one verification of identity, determining whether an individual is who they purport to be. A live profile can be compared with a template stored in the computer system or identification document, such as a passport or licence. Biometric identification can also be used is to identify individuals on a watch-list, such as by screening closed circuit television footage with facial recognition technology (Smith et al., 2018).

Individual biometrics have strengths and weaknesses, depending on the context in which they are used. Seven criteria have been accepted as key indicators of the suitability of biometric features: universality, distinctiveness, permanence, collectability, performance, acceptability, and resistance to circumvention (Jain et al., 2006) (Table 1.1). For example, fingerprinting or facial recognition may be selected

over gait analysis at passport control; but when analysing television footage to identify a suspect, gait analysis may be preferred because it can be assessed from a greater distance and obtaining fingerprints from such a large group of people would not be feasible. Ideally, facial recognition could be combined with gait analysis to provide a higher degree of accuracy.

1.2 The First Biometric: Fingerprint Identification

The technique of fingerprint identification, in both analogue and digital forms, is based on differences within the standard patterns of the ridges. These can be classified into a series of arches, loops and whorls. The centre of a pattern is referred to as the core, and points of deviation referred to as the delta. The points of discontinuity in a fingerprint, where a ridge branches or ends, are known as minutiae. Approximately 30 minutiae are used in the fingerprinting technique. Fingerprinting has advanced significantly with digitalisation in the twenty-first century. Optical scanners and algorithms are now used to record, digitally retrieve and match fingerprint data; in contrast with the initial manual, card-based system. Automated fingerprint databases of hundreds of millions of people have now been established. These are fully automated, or only require human input at the final stage to distinguish between highly similar fingerprints as part of a list of close matches to an unknown suspect in a law enforcement investigation (Moses et al., 2010).

Since the mid-2000s, fingerprint identification has been widely used outside law enforcement, with the first major development being the integration of biometric fingerprint identification (along with facial recognition) into passports and border control systems. This was made a requirement for foreign nationals and visa applicants in many countries, including the United States in 2004, Japan and the United Kingdom in 2008, the European Union in 2011, and Canada in 2013 (Canadian Government, 2017). It is also widely used across Africa, the Middle East and Asia. Non-government organisations, such as the Office of the United Nations High Commissioner for Refugees (UNHCR), also use fingerprint identification to identify refugees in aid programs, using portable, battery powered devices in remote settings (Lodinová, 2016). Perhaps the largest fingerprint identification database is the government administered Aadhaar database in India, which includes more than 1.2 billion people for public administration purposes (Saferstein, 2015).

Over the past decade, fingerprint identification has been widely used outside law enforcement and government. This includes for employee attendance and building access control; and in personal devices such as smartphones and laptops. The introduction of fingerprint scanning capabilities into smartphones has provided an opportunity to apply fingerprint identification into a broader range of commercial applications – it is now common for personal banking to be undertaken online with biometric fingerprint identification. Other developing applications of fingerprint identification include within the handpiece of a firearm to ensure that it can only be

Table 1.1 Key indicators of the suitable biometric features

Universality	Distinctiveness	Permanence	Collectability	Acceptability	Performance	Resistance to circumvention
The biometric should be present in all individuals.	The biometric feature should be sufficiently different to distinguish between individuals.	The biometric feature should be unchanged over the individual's life.	The degree of ease of collecting and measuring the biometric.	The extent to which an individual or society accepts the use of the biometric feature as a means of identification.	The degree of accuracy and the speed of the system.	The extent to which the system can be bypassed or defeated.

used by the registered owner. It is being deployed by government in relation to firearms for police and military personnel to improve safety (Simonetti et al., 2017).

Biometrics are arguably a more accurate and convenient means of recording employee attendance than traditional methods such as punch clocks or swipe cards, and as costs have decreased, they have become increasingly common. In the case *Jeremy Lee v. Superior Wood Pty Ltd,*[1] a sawmill company implemented fingerprint scanners to record employee attendance. When one employee refused to provide his fingerprint and was subsequently dismissed, litigation ensued resulting in litigation over the fairness of their dismissal on that basis. On appeal it was held that because biometrics were classified as sensitive information under privacy law, consent was required to collect this information. Without it, the direction to use the scanners was not a 'lawful and reasonable direction' and Mr Lee's failure to follow the direction was not a valid reason for dismissal. This issue for employers can be addressed by making the collection of biometric data a condition of employment that would need to be accepted prior to commencing work (Holland & Tham, 2020).

Biometric fingerprint databases, known as Automated Fingerprint Identification Systems (AFIS), were first established in the late 1990s, and these continue to be a primary method of establishing identity in law enforcement and border protection contexts. Law enforcement systems include a standardised ten-print holding of fingerprints obtained under controlled conditions from a suspect during the course of an investigation, or following arrest; as well as latent fingerprints (formed from traces of sweat, oil or other substances on the surface of the skin) obtained from crime scenes or items physical evidence. Latent fingerprints are typically of lower quality and may only include a partial print (Milne, 2013).

A range of biometric fingerprint databases have been established around the world. The United States introduced the Integrated Automated Fingerprint Identification System (IAFIS) in 1999, transitioning to the multimodal Next Generation Identification (NGI) system in 2011, which also includes photographs, facial templates and criminal history and intelligence data. The NGI is operated by the Federal Bureau of Investigation (FBI) and provides services to federal, state and local law enforcement and national security agencies throughout the United States (FBI, 2017). The national fingerprint database in the United Kingdom is known as IDENT1. A key difference in this jurisdiction is that the database was developed as a joint venture between the Home Office and the defence technology company Northrop Grumman in 2004. It provides a link between law enforcement agencies across England, Wales and Scotland, as well as records in the Police National Computer (Northrop Grumman, 2017). In Australia, the national biometric fingerprint database has operated since 2001. The National Automated Fingerprint Identification System (NAFIS) provides Australian law enforcement, security and border agencies, with a centralised national database for finger and palm print images (ACIC, 2020). Data sharing arrangements have been established between these countries, as well as Canada and New Zealand (Canadian Government, 2017).

[1] [2019] FWCFB 2946.

The digitisation of fingerprint identification through automated databases has led to a significant increase in positive identifications and linkages between individuals and physical evidence at other crime scenes, enhancing the efficiency of investigations. An evaluation of the fingerprint database in the United Kingdom examined the collection of fingerprint evidence in relation to volume crimes, such as burglary and motor vehicle thefts, demonstrating a greater capacity to identify suspects as well as faster case outcomes (Saferstein, 2015). Despite new forms of biometrics being developed, fingerprint identification continues to play an important and growing role in law enforcement. Figures from Australia indicate a significant expansion in database searches over the past decade. For example, in the 2007–2008 financial year, there were approximately 300,000 searches for fingerprints on the national database, and by the 2018–2019 financial year this had increased to more than 1.5 million searches (ACIC, 2019).

The legal system plays an important role in evaluating and regulating evidence such as biometric fingerprints – this form of identification evidence can have a significant bearing on the outcome of proceedings. As discussed, crime scene examiners may obtain 'latent' fingerprints or palm prints on objects, which can link a defendant to a crime. Over the past century courts have routinely admitted fingerprint evidence.[2] Evidence of a fingerprint match would be presented by the investigating police officer with specialised knowledge of fingerprinting techniques, or a forensic scientist who collected and compared the prints.[3]

Identification evidence is circumstantial, and the probative value of a fingerprint match must be assessed in the context of the other evidence in a criminal trial; but it will be of greatest value to the prosecution if there is no innocent explanation for its presence at a crime scene. Obtaining fingerprints at a crime scene and comparing them using a database and the specialist knowledge of a forensic scientist is regulated by forensic procedures legislation. Collecting fingerprints from a suspect is regulated by criminal procedure legislation – generally, there must be reasonable grounds for believing that requiring a suspect to provide their fingerprints would be necessary for identifying the person responsible for a sufficiently serious offence, and if that requirement is satisfied, they may be obtained without the suspect's consent.[4]

The comparison of fingerprints involves the identification of numerous minutiae within the print.[5] The more points that are compared, and the greater the degree of similarity, the more persuasive the inference that can be draw regarding identity. The comparison of fingerprints differs from other forms of biometrics, such as DNA identification in that it does not involve the calculation of a match probability that two samples came from the same individual. It is based on human judgment in

[2] *Parker v R* [1912] HCA 29; (1912) 14 CLR 681, Griffith CJ at 683, cited in *R v Mitchell* [1997] ACTSC 93; (1997) 130 ACTR 48 (18 November 1997).

[3] See, for example, *DPP v Watts* [2016] VCC 1726 (23 November 2016).

[4] Section 3ZJ, *Crimes Act 1914* (Cth).

[5] *JP v Director of Public Prosecutions (NSW)* [2015] NSWSC 1669 (11 November 2015), [36].

making a visual comparison, aided by a database and algorithm, rather than a statistical calculation (Edmond, 2015).

Expert evidence law provides that a witness with specialised knowledge must be able to explain how identification evidence provides a sound basis for the conclusions they draw about the evidence.[6] To the extent that any of the evidence is unclear, the defence may seek to have it excluded, or ask for the jury to be cautioned regarding the weight they accord it.[7] Judges must consider that a jury hearing, for example, that the defendant's fingerprints were matched to a crime scene using a police database, may infer that the defendant has a criminal history. The defence could seek to exclude evidence as unfairly prejudicial or seek to have the judge to warn the jury against making an adverse inference on that basis.

1.3 Applied Ethics

Issues in applied ethics, including many public policy issues, have a value dimension as well as a scientific dimension. The value dimension is in need of systematic analysis and illumination by way of moral theories and perspectives. Here it is not simply a matter of philosophical theory being mechanically applied to specific problems; rather there is a complex interplay between theoretical perspectives, on the one hand, and specific ethical intuitions and concrete scientific data, on the other. For example, whether or not biometric identification constitutes an infringement of the right to privacy, is partly a matter of figuring out what is important about privacy (the ethical theory of privacy) as well as knowing the scientific facts about the particular biometric in question and the uses to which it is put by, for instance, law enforcement. Further, it may well be a matter of balancing the moral weight to be given to privacy against the benefits delivered by these databases in the specific contexts in question. On the other hand, it may well call for creative thinking of a kind that would enable us to possess integrated databases without necessarily infringing the right to privacy. For example, such databases might be able to be designed in such a way that access was available only to certain persons under highly restricted circumstances, e.g. law enforcement officials possessed of a judicial warrant in the circumstance of a very serious crime. That is, our agreed ethical perspective on this issue could be designed-into the technology or the institutional, including legal, arrangements (van den Hoven et al., 2017).

The philosophical theory itself operates at a number of levels of abstraction. There are high level theoretical claims, such as the principle of maximizing the satisfaction of the greatest number or seeking to benefit the least advantaged

[6] Leading authorities on specialized knowledge under UEL s79(1) are *Makita (Australia) Pty Ltd v Sprowles* [2001] NSWCA 305 (14 September 2001); *HG v The Queen* [1999] HCA 2; 197 CLR 414; and *Honeysett v The Queen* [2014] HCA 29; 253 CLR 122.

[7] In *JP v Director of Public Prosecutions (NSW)* [2015] NSWSC 1669 (11 November 2015); *Dasreef Pty Ltd v Hawchar* [2011] 243 CLR 588.

(Alexandra & Miller, 2009a). But there are also lower level philosophical theories of specific values, e.g. an ethical theory of scientific freedom, or of a specific occupational role, e.g. an ethical theory elaborating the moral purpose and characteristic virtues of a criminal investigator or of a forensic scientist (Miller & Gordon, 2014). These lower-level normative or value theories operate within specific institutional, occupational and technological settings; they are context dependent. As such they grow out of, and are highly sensitive to, specific situations and problems.[8]

Much of the philosophical work on ethics undertaken in universities in the English-speaking world in the last century was concerned with higher order abstract theory, as opposed to lower order context dependent theory. However, it has become clear that lower order context dependent theory is back on the agenda under the heading of applied ethics. Moreover, arguably, higher order abstract theory in so far as it is purely formal (value formalism) is of little assistance in the solution of practical ethical problems. Consequentialism and formalist deontological theories are species of value formalism. (Consequentialism is, roughly speaking, the theory that one should always act in such a way as to maximise the good consequences of one's action; neo-Kantian formalist deontological accounts are erected on a principle of universalizability, i.e. only perform an action in a situation if you can consistently will everyone to perform the action in that situation.) Here we must distinguish between value formalism and substantive ethical theories. Bernard Gert offers a substantive ethical theory in this sense (Gert, 2004; Alexandra & Miller, 2009b). According to Gert there are ten moral rules, which fall into two groups. The rules in both groups instruct us not to act in ways which will cause the five basic harms rational persons want to avoid, death, pain, disability, loss of freedom, and loss of pleasure. The first five moral rules are: Do not kill; Do not cause pain; Do not disable; Do not deprive of freedom; Do not deprive of pleasure. These rules prohibit those kinds of actions that *directly* cause these harms. The second five rules are: Do not deceive; Keep your promises; Do not cheat; Obey the law; Do your duty. These rules prohibit those kinds of actions that *indirectly* cause the five basic harms. Arguably, Gert's list both omits some basic moral principles, and includes some that ought not to be included. Perhaps the two most obvious omissions from the list are 'Do not steal or damage other people's property' and 'Do not defraud'.

Moreover, Gert was apparently wrong to include as a basic rule that we should obey the law since perhaps there is a moral obligation to obey *specific* laws and *specific* legal systems, but only because those laws/legal systems embody the moral rules and/or achieve collective goods not otherwise obtainable. On this account legal systems or laws as such do not generate moral obligations, even presumptive

[8] This need to relativise moral theories, perspectives and principles to institutional and technological context does not imply relativism, i.e. the theory that moral statements are not objectively true. The proposition that killing is wrong stands in need of relativisation. In general, it is morally wrong to kill another human being. However, in some contexts, e.g. in a situation of self-defence, it is morally permissible. However, from the fact that moral principles need to be relativised to context, it does not follow from this that the moral claims implicit in such relativisation are not objectively true (Alexandra & Miller, 2009a Ch. 2).

moral obligations that can be overridden. So the obligation to obey the law is entirely unlike the obligation to keep one's promises. Other things being equal, making a promise creates a moral obligation. Naturally, some promises – such as a promise to kill innocent people – do not create obligations, and some promises that do create moral obligations can be overridden in certain circumstances. However, other things being equal, the fact that there is an extant legal system prescribing a particular set of acts and omissions does not entail that there is an obligation to obey those laws; rather it all depends on the laws in question, or so it could be argued. At any rate, in this work we will be making some suggestions in relation to what particular laws there ought to be in relation to different biometric technologies and their uses.

To return to substantive ethical theories: they provide an ethical framework that can usefully inform practical ethical decision-making. For this reason, it is important to utilize substantive theories and, in particular, some of their constitutive moral principles, e.g. do not deprive persons of their freedom. However, in doing so further analysis of often called for in respect of the content of these principles, e.g. the concept or, better, concepts of freedom in play. By contrast, it would seem that value formalist theories are in themselves simply too abstract to provide ethical guidance; at best they rule out certain combinations of action on the grounds of inconsistency (e.g. actions that fail the universalizability test) or unhelpfully state the obvious (e.g. 'Always take into account the consequences of your actions'). Naturally, this inadequacy of formalist theories can be addressed by providing in some other way this missing content, e.g. by drawing up a list of the good consequence to be pursued. However, this manoeuvre simply draws attention to the need for a substantive ethical theory, e.g. a theory that specifies the goods or content-laden principles in question. But the lack of such as substantive ethical theory is precisely what we do not have, and what formalist theory cannot give us. Moreover, once we have the substantive theory, there is hardly any role left for formalist theory in relation to practical ethical decision-making, or so we suggest.

1.4 Collective Moral Responsibility

The development of biometric technology, such as fingerprinting, by scientists and others, and its uses by individuals within government agencies and law enforcement, e.g. for criminal investigations, is a complex undertaking involving multiple organizations and numerous individuals. Accordingly, the activities engaged in and their outcomes are a matter of collective responsibility and, since these activities and outcome are often morally significant, collective moral responsibility. However, the notion of collective moral responsibility is itself complex, especially as it applies to such a network of interconnected activities as this.

The notion of collective moral responsibility that we will be using in this work is that of joint moral responsibility (Miller, 2001a Ch. 8, 2006, 2010 Ch. 4). Collective moral responsibility is a species of moral responsibility and contrasts, in particular,

with individual moral responsibility. However, the notion of moral responsibility, whether individual or collective, contrasts with a number of other notions.

First, we need to distinguish moral responsibility (including collective moral responsibility) from causal responsibility. A person or persons can inadvertently cause a bad outcome without necessarily being morally responsible for so doing. For example, a careful and competent fingerprint expert who is obeying all the relevant regulations and best practice procedures might, nevertheless, incorrectly judge that there is a match between the fingerprints of a suspect and the fingerprints found at the crime scene leading to the arrest of an innocent person because the fingerprint sample he used was the wrong one due to an error in the chain of custody of evidence.

Second, we can distinguish moral responsibility from what can be referred to as natural responsibility. Moral responsibility typically requires not only causal responsibility but also an intention to cause good or evil (or at least the knowledge that one's action will or may well cause good or evil) and an intention that is itself under one's control. On the other hand, one is not necessarily *morally* responsible for one's actions under one's control since such action might not have any moral significance. If a fingerprint expert makes himself a cup of coffee then under normal conditions he is responsible for doing since the action is entirely under his control; however, arguably, he is not *morally* responsible for doing so, given the action of making a cup of coffee has no moral significance.

Third, we need to distinguish moral responsibility from institutional responsibility, e.g. legal responsibility. An investigator might be morally responsible for breaking her promise to a suspect without being legally responsible, or otherwise institutionally responsible, for so doing.

As is the case with individual responsibility we can distinguish between collective moral responsibility, on the one hand, and collective causal, collective natural and collective institutional responsibility, on the other hand. Collective moral responsibility is the moral responsibility that attaches to the members of both structured and unstructured groups of human persons for their morally significant actions and omissions. Organizations, e.g. security agencies, are structured groups and their members can be held collectively morally responsible for the outcomes of their joint actions, e.g. the reduction of crime.

According to the theory of collective responsibility as joint responsibility, at least one of the central senses of collective responsibility is responsibility arising from joint actions (and joint omissions (Miller, 2001b)). Roughly speaking, a joint action can be understood thus: two or more individuals perform a joint action if each of them intentionally performs an individual action but does so with the (true) belief that in so doing each will do their part and they will jointly realise an end which each of them has and which each has interdependently with the others (a collective end) (Miller, 1992, 1995, 2001a Ch. 2). Thus, the members of a major serious crime investigation team investigation a murder, comprised of investigators, forensic experts and so on might identify and arrest an offender or, perhaps, offenders (Miller, 2014, 2015). Since the realization of this end is the result of the interdependent action of individual actions of the investigators (e.g. those who interviewed

suspects, those who collected fingerprints), forensic experts (e.g. those who searched an automated fingerprint database and verified a match to a suspect), et al, it is a joint action and the end realized is a collective end. Moreover, since the identification and arrest of those who have committed serious crimes is morally significant, the members of the investigation team in question can be held to be collectively, i.e. jointly, morally responsible for this outcome (and as morally praiseworthy).

On this view of collective responsibility as joint responsibility, collective responsibility is ascribed to individuals. Each member of the group is individually morally responsible for his or her own contributory action, and (at least in the case of most small scale joint action – see below) each is also individually (fully or partially – see below) responsible for the aimed at outcome, i.e. the realised collective end, of the joint action. (We note that an outcome of a joint action might not be aimed at and, if so, it is not a constitutive element of a successful joint action, i.e. it is not the realized collective end of the joint action.) However, each is individually responsible for the realized collective end, *jointly with the others*; hence the conception is relational in character. Thus, in our above criminal investigation example, a member of the forensic team who collected fingerprints at the crime scene is ultimately responsible jointly with the other members of the investigation team (including the other forensic experts) for identifying the offenders because she performed her contributory action in the service of that collective end; the same point holds for each of the other members of the criminal investigation team. And, to reiterate, if the joint action had no moral significance then the participants would have had joint *natural* responsibility for their action but not joint, i.e. collective, *moral* responsibility for it. However, since the joint action in question is a morally significant action then, as mentioned above, the members of our forensic team are jointly (collectively) *morally* responsible for the outcome.

We note that on the theory of collective responsibility as joint responsibility it is possible that while each participant in a morally significant joint action makes a causal contribution to the aimed at outcome of the joint action, none of these contributing actions considered on its own is either necessary or sufficient for this outcome. Suppose that in a murder investigation, the forensic team provides multiple pieces to forensic evidence, e.g. fingerprints of the suspect at each of a number of connected crime scenes, including at the murder location, on threatening letters sent to the victim prior to the crime etc. None of these sets of fingerprints on it is own is either necessary or sufficient to secure the conviction of the offender, let us assume, however each set adds evidential weight to the case against the offender. Therefore, each of the members of the forensic team has some responsibility jointly with other members of the investigation team (including the other members of the forensic team) for the conviction. That is, each has a share of the collective moral responsibility for the outcome; a share jointly held with the others.

Notice that each of the members of the forensic team has only partial moral responsibility (held jointly with the others); none has full moral responsibility. This is often so in instances of joint action in which the contributing action of each is neither necessary nor sufficient for the outcome and almost always so in epistemic (or knowledge-based) joint action; and, therefore, in forensic work. However, we

should note that it is not necessarily so in cases of kinetic joint action of a serious criminal nature, i.e. it is by no means necessarily true of the criminal actions which members of forensic teams investigate. Suppose that in our murder investigation example there were six offenders. Assume the six men simultaneously (deliberately and without moral justification) stabbed a seventh (innocent) man, and each does so having as an end to kill their victim. However, each knows that his one act of stabbing will only wound the victim, and that four stabs wounds taken together are necessary and sufficient to kill the victim. We further note that on this theory it is possible that in such scenarios – scenarios in which each participant makes a causal contribution which is neither necessary nor sufficient for the outcome – each participant is *fully* morally responsible (jointly with the others) for the outcome. Consider, for instance, our stabbing scenario. Firstly, each of the six men is individually fully morally responsible for the stab wound he inflicted. Secondly, the six men are jointly morally responsible for killing the man, i.e. they are jointly responsible for murder. Significantly, in relation to this joint responsibility, each of the six is *fully* morally responsible (jointly with the other five) for the murder (and, assuming there was sufficient evidence, each would in all likelihood be held criminally responsible for murder).

What of large-scale morally significant joint actions and omissions, such as the creation of a national database of fingerprints in the service of the collective good of security (Miller, 2010 Ch. 2, 2018)? These introduce a range of issues which are often not present in small scale, morally significant joint actions and omissions. For one thing, large-scale cases often involve hierarchical organizations and hence the potential for those in subordinate positions having diminished moral responsibility. For another thing, the extent of the contribution to the outcome of a joint action or omission can vary greatly from one participant to another. Indeed, some of those who make a causal contribution to a joint action – and especially to large-scale joint actions – might, nevertheless, not be genuine participants in that joint action because in performing their contributory action they were not aiming at the outcome constitutive of the joint action; some did not have its collective end as their end. On the theory of collectively responsibility as joint responsibility, the members of a number of forensic teams (together with members of other teams such as members of computer database teams who input data etc.) can be ascribed collective moral responsibility, at least in principle, for the national fingerprint database to the extent that they acted jointly with one another, (i.e. members of a given team with other members of that team, and the membership of one team with the membership of other teams[9]) in ways that led to its creation. Here the network of joint actions could be quite wide and complex without involving (either causally or in terms of their intentions, ends or responsibilities) all, or even most, members of all forensic teams, computer database teams, etc. Moreover, some joint actions or omissions are likely to be of greater moral significance than others, and some individual contributions,

[9] This notion of one team acting jointly with other teams involves a multi-layered structure of joint action. See Miller, 2001a, pp. 173–5, 2010, pp. 48–50, 2018.

e.g. those of the managers, of greater importance than others, e.g. those of lower echelon employees.

It is important to note here that not only is each agent individually (naturally) responsible for performing his contributory action, each is responsible by virtue of the fact that he intentionally performs this action (and his intention is under his control and connects to his action in the right way), and the action is not intentionally performed by anyone else. Of course, the other agents (or agent) *believe* that he is performing, or is going to perform, the contributory action in question. But mere possession of such a belief is not sufficient for the ascription of responsibility to *the believer* for performing the individual action in question. So, what are the agents *collectively* (naturally) responsible for? As already mentioned, the agents are collectively (naturally) responsible for the realization of the (collective) *end* that results from their contributory actions.

Consider each member of the above-mentioned major crime investigation team (Miller, 2014, 2015). Assume that while each investigator who (say) interviewed a suspect and each forensic expert who scrutinized some fingerprints, made a direct or indirect contribution to the ultimate outcome, i.e. the identification and arrest of the offenders, nevertheless, some of these actions were redundant or otherwise not causally necessary for the outcome. For instance, some initial suspects were eliminated because their fingerprints did not match those at the crime scene yet their elimination was not, as it turned out, necessary for the outcome. Therefore, the actions of a *subset* of the criminal investigation team was sufficient for the outcome; so although the actions of each and every member of the investigation team made a contribution, the actions of some of the members were not necessary (or, obviously, sufficient) to realize the collective end. Evidently, as already noted above, in joint actions (as opposed to joint omissions), while each single constitutive individual action needs to make a contribution, none needs to be causally or otherwise necessary to realize the relevant collective end.

This theoretical point has an important implication for the ascription of collective (i.e. joint) moral responsibility to participants in morally significant, large-scale joint actions, in particular, since typically in large-scale joint actions no contribution of a single participant taken on its own is necessary in order to realize the collective end of the joint action. Specifically, it is now possible, at least in principle, to ascribe collective, i.e. joint, moral responsibility to participants in morally significant, large-scale joint actions, such as a major crime investigation (Miller, 2001a Ch. 5, 2010 Ch. 1, 2014, 2015). The fact that in a large-scale joint action the action of each participant taken on its own is not necessary to realize the collective end of the joint action is not, given this theoretical point, a barrier to the ascription of moral responsibility to each participant (jointly with the others) for the realization of this collective end. Note that it does not follow from this that each participant in a large-scale joint action is *fully* morally responsible (jointly with the others) for the realization of the collective end of the joint action, e.g. the arrest of a large number of offenders in a major crime investigation. Indeed, this is unlikely given that the causal contribution of each in large-scale joint actions is often very small and the commitment of each to the collective end correspondingly very weak. Rather in such cases each

might only have *partial* moral responsibility (jointly with the others), or perhaps a *share* in the moral responsibility, for the realization of the collective end.

1.5 Fingerprinting: Key Ethical Issues

Fingerprint identification techniques conveniently exemplify many of the ethical issues raised by biometric identification methods discussed in this book and, in particular, DNA, facial recognition technology and biometric databases. That said, for the most part fingerprint identification techniques raise these issues in a less acute form. This is because fingerprint identification (including, therefore, databases of fingerprints) is arguably less invasive of privacy and, therefore, less invasive of autonomy than DNA and facial recognition technology. The inherited nature of DNA means there are potentially implications beyond the identification of single individuals, and further, DNA can also potentially be analysed to obtain health and other information; while facial images can be more readily obtained than fingerprints, such as through CCTV, or from online searches.

Here it is important to distinguish the process by which fingerprints (or other biometric data) might be obtained and the right to control one's biometric data. The process of acquiring fingerprints might need to be coercive, e.g. in relation to an offender who resists providing his fingerprints to police, though they may also be freely given to a technology company or financial institution in order to utilise them as a security feature of a device or account. However, it does not follow from this that the possession of one's fingerprints is more invasive than, for instance, the possession of one's DNA.

On the other hand, from a law enforcement and security perspective, arguably fingerprint identification techniques (and databases of fingerprints) are less powerful than DNA and facial recognition technology (and their respective databases), although as discussed above, different biometrics may be more or less relevant or useful depending on the context, or used in unison to provide greater confidence in an identification. DNA traces are more ubiquitous and more reliable than fingerprints. Facial images (once made) can be more effectively used for identification purposes than fingerprints since identification via fingerprints relies essentially on databases of fingerprints whereas facial images, in addition to being stored in databases (e.g. of drivers' licenses), are communicable to the population at large (e.g. via TV news) and searchable on social and other media. Moreover, facial recognition technology provides a powerful tracking mechanism (e.g. via networks of CCTV cameras) (Smith et al., 2018).

Biometric databases, whether of fingerprints, DNA or facial images, are an increasingly important law enforcement and national security tool for intelligence, investigative and evidential purposes but, as already mentioned, they raise ethical issues. However, it is the interlinking of biometric databases with one another and with non-biometric databases (e.g. health and financial databases) that provides the most powerful law enforcement and national security tool but which also raises the

most profound ethical concerns. Here the spectre of an authoritarian 'big brother' state looms, of which contemporary China is increasingly being seen as an exemplar.

What are the ethical or moral (we use these terms interchangeably) issues raised by biometric technologies, including both moral benefits as well as moral costs? The most obvious are: (1) privacy and, relatedly confidentiality and individual autonomy; (2) security, e.g. against terrorism and organized crime; (3) power imbalances, e.g. between the government and the citizens; (4) democratic accountability. Additional ethical or moral issues that are perhaps less obvious include the moral right to ownership of one's genetic data, the right not to self-incriminate, and the collective moral responsibility on the part of members of the citizenry to combat crime (or, at least, to assist law enforcement to do so). Three overarching moral issues are, firstly, as we have just seen collective responsibility for the collective good of security and, therefore, to establish, for instance, fingerprint databases; secondly, the liberal-democratic state and the preservation of its constitutive values and; thirdly (and, relatedly), the so-called dual use dilemma in relation to new and emerging technology (in this instance, biometrics). Dual use dilemmas arise in relation to new and emerging technologies as a result of the potential conflict between, on the one hand, the extraordinary actual or potential benefits they confer e.g. in crime reduction and, on the other hand, the actual and potential harms they cause, e.g. infringements, if not violations, of moral rights to privacy and autonomy.

Considered on its own, the use of fingerprint technology by law enforcement and national security agencies seems relatively morally unproblematic, at least under certain conditions, e.g. if fingerprint collection is restricted to crime scenes and fingerprint databases consist only of the fingerprints of those convicted of crimes or reasonably suspected of crimes. In addition, epistemic concerns need to be addressed, e.g. chain of custody of evidence, prints are of good quality and judgements thereof that are used in criminal trials are made and scrutinised by appropriately qualified and experienced experts, and even then considered in the context of other relevant evidence.

However, fingerprint technology is now used by many countries at national borders and, therefore, to reliably identify travelers, irrespective of whether they have criminal convictions or are suspected of any crime (they are now widely used as a security feature in a broad range of civilian contexts). Such use might be justified in terms of border protection and, therefore, national security, albeit on the condition that it not be used for other purposes and that it be subject to stringent accountability mechanisms. The argument here might have recourse to the collective good of security (Miller, 2010 Ch. 2) to which each traveler ought to be prepared to make a contribution by providing fingerprint. They ought to make a contribution because they enjoy the collective good (the security) that is provided by the database of fingerprints. To enjoy this security and yet refuse to allow one's fingerprints at the border would be to unfairly free-ride. Of course, free-riding might be justified if the costs borne were greater by some individuals or were violations of rights and, specifically, in the case of fingerprints, the right to privacy and/or autonomy. On the other hand, an individual can sometimes be expected to bear a minor cost for the

sake of the greater good, even if the individual does not personally benefit from that good (Miller, 2010, pp. 337–8).

As mentioned above, and will become clearer in later chapters, fingerprint technology may be considered less invasive than, for example, facial recognition technology. One may not as easily claim ownership of one's fingerprints in the sense of the impressions one's fingers leave on certain surfaces in comparison with a claim that they own or, at least, should have some rights with respect to, photos taken of one's face. Perhaps because although one's face is more visually accessible to others than the patterns on the skin of one's fingers, one's face is constitutive of one's personal identify in a more profound sense than patterns on the skin of one's fingers. The latter may enable a person to be uniquely identified but they do not significantly contribute to a person being who they are.

Given fingerprint technology is an effective tool in law enforcement and in the service of national security, including for purposes of border protection, and given there is no less invasive technology available and fingerprint technology is not particularly invasive, it seems that the argument from the collective moral good of security and, therefore, the existence of a collective moral responsibility to establish fingerprint databases and use fingerprint technology, and the concomitant moral obligation not to free-ride, is persuasive. However, it is important to note that this argument does not demonstrate that *universal* fingerprint databases ought to be established. For one might be under a moral obligation to provide one's fingerprint for exculpatory purposes in relation to a specific crime only; in which case storage in a universal database (as opposed to a database of the fingerprints of those who have committed a crime or are currently suspected of doing so). Naturally, there are other security purposes, e.g. border control, that would justify a database of travelers but again this is short of a universal database and might require a warrant if it were to be accessed for other purposes.

A further set of related questions arise as to whether the use of fingerprint technology can be morally justified outside criminal justice or national security contexts, e.g. in the private sector. Presumably, fingerprint technology could be justified in circumstances in which those whose fingerprints were being used had given their consent in the following strong sense of consent. Here it is important to note that *strong* consent (which may extend further than the legal requirements of consent or than the requirements of weaker non-legal definitions) to an action necessitates that: (i) the agent of the action is a rational adult who intentionally performs the action; (ii) the agent is reasonably well-informed regarding the action; (iii) the action is optional in the sense that the agent can choose not to perform it (as might not be the case if the agent is coerced); (iv) the agent in choosing the action is not being *unjustly* deprived of some *essential* good or service to which the agent has a *moral right*, as might be the case if the agent could not have a bank account or use a computer unless the agent consented (in some weaker sense) to the use of fingerprint technology to access the account or to use the computer. However, the use of fingerprint technology might be morally justified in the private sector, as in the public sector, if the moral weight of the collective good which it served overrode the individual rights infringed and, in particular, if the collective good of security overrode

the privacy rights infringed. Consider, for example, the health records held in a private sector database which might be vulnerable to hacking and, therefore, ransomware attacks unless stringent security measures were in place, including the use of the biometric identification technique of fingerprinting. On the other hand, there would need to be assurances that the database of fingerprints was itself secure. For if not its value as a protective measure in relation to health records may well be greatly reduced.

1.6 Conclusion

The development of biometric identification began with a classification system for fingerprints in the mid-nineteenth century and was quickly applied to legal contexts, such as criminal investigation. Today, along with DNA identification and facial recognition, biometric applications are not only used in law enforcement, but have expanded to other areas of society, such as security access in personal devices such as smartphones. Applied ethics plays a key role in determining and justifying how these expanding uses should be regulated by law, providing systematic analysis of the associated values, such as balancing the moral weight to be given to privacy against the benefits delivered by biometric databases in the specific contexts. We argue that the use of biometric technology for certain limited purposes and contexts are a matter of collective moral responsibility and illustrated this using the actors involved in using fingerprint evidence in a criminal investigation. However, we argued that this collective moral responsibility does not extend to the creation of universal fingerprint databases or the accessing of a database justifiably established for one purpose, (e.g. a database of the fingerprints of holders of a bank account), being accessed for another purpose (e.g. by law enforcement officers) without an adequate justification (and in compliance with appropriate legal accountability measures, such as a judicial warrant). We note that fingerprint identification technology is likely to be less morally problematic than other biometrics, such as facial recognition and DNA identification, and that their use, in public or private sector settings can be justified in circumstances in which more invasive technologies are not. Relevant factors in this assessment include the existence of strong consent (as defined above), and where the moral weight of the collective good of security overrode the privacy rights infringed.

References

Alexandra, A., & Miller, S. (2009a). *Ethics in practice: Moral theory and the professions*. UNSW Press.

Alexandra, A., & Miller, S. (2009b). Ethical theory, 'Common Morality' and professional obligations. *Theoretical Medicine and Bioethics, 30*(1), 69–80.

Allen, R., Sankar, P., & Prabhakar, S. (2005). Fingerprint identification technology. In J. L. Wayman, A. K. Jain, D. Maltoni, & D. Maio (Eds.), *Biometric systems: Technology, design and performance evaluation* (pp. 22–61). Springer.
Ashbourn, J. (2000). *Biometrics: Advanced identity verification*. Springer.
Australian Criminal Intelligence Commission (ACIC). (2019). *Annual report 2018–2019*. Australian Government.
Australian Criminal Intelligence Commission (ACIC). (2020). *Biometric and forensic services*. https://www.acic.gov.au/services/biometric-and-forensic-services
Canadian Government. (2017). *International use of biometrics*. http://www.cic.gc.ca/english/department/biometrics-international.asp
Edmond, G. (2015). Forensic science evidence and the conditions for rational (jury) evaluation. *Melbourne University Law Review, 39*, 77–121.
Federal Bureau of Investigation (FBI). (2017). *Integrated automated fingerprint identification system*. http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis
Gert, B. (2004). *Common Morality*. Oxford University Press.
Holland. P., & Tham T. (2020, April). Workplace biometrics: Protecting employee privacy one fingerprint at a time. *Economic and Industrial Democracy*, 1–15.
Hopkins, R. (1999). An introduction to biometrics and large scale civilian identification. *International Review of Law, Computers and Technology., 13*, 337–363.
Jain, A., Ross, A., & Pankanti, S. (2006). Biometrics: A tool for information security. *IEEE Transactions on Information Forensics and Security, 1*(2), 125–143.
Lodinová, A. (2016). Application of biometrics as a means of refugee registration: Focusing on UNHCR's strategy. *Development, Environment and Foresight, 2*(2), 91.
Miller, S. (1992). Joint action. *Philosophical Papers, XXI*(3), 275–299.
Miller, S. (1995). Intentions, ends and joint action. *Philosophical Papers, XXIV*(1), 51–67.
Miller, S. (2001a). *Social action: A teleological account*. Cambridge University Press.
Miller, S. (2001b). Collective responsibility and omissions. *Business and Professional Ethics, 20*(1), 5–24.
Miller, S. (2006). Collective moral responsibility: An individualist account. *Midwest Studies in Philosophy, XXX*, 176–193.
Miller, S. (2010). *The moral foundations of social institutions: A philosophical study*. Cambridge University Press.
Miller, S. (2014). Police detectives, criminal investigations and collective responsibility. *Criminal Justice Ethics, 33*(1), 21–39.
Miller, S. (2015). Joint epistemic action and collective responsibility. *Social Epistemology, 29*(3), 280–302.
Miller, S. (2018). Joint epistemic action: Some applications. *Journal of Applied Philosophy, 35*(2), 300–318.
Miller, S., & Gordon, I. (2014). *Investigative ethics: Ethics for police detectives and criminal investigators*. Wiley-Blackwell.
Milne, R. (2013). *Forensic intelligence*. CRC Press.
Moses, K., Higgins, P., McCabe, M., Probhakar, S., & Swann, S. (2010). Automated fingerprint identification system. In *Fingerprint Sourcebook*. National Institute of Justice.
Northrop Grumman. (2017). *IDENT1 automated fingerprint system, United Kingdom*. http://www.homelandsecurity-technology.com/projects/ident1-automated-fingerprint-system-northrop-grumman-uk/
Saferstein, R. (2015). *Criminalistics: An introduction to forensic science*. Pearson Education.
Simonetti, J., Rowhani-Rahbar, A., & Rivara, F. (2017). The road ahead for personalized firearms. *JAMA Internal Medicine., 177*(1), 9–10.
Smith, M. (2016). *DNA evidence in the Australian legal system*. Lexis Nexis.
Smith, M., Mann, M., & Urbas, G. (2018). *Biometrics, crime and security*. Routledge.
Van den Hoven, J., Miller, S., & Pogge, T. (2017). *Designing-in-ethics*. Cambridge University Press.

Chapter 5
The Future of Biometrics and Liberal Democracy

Abstract The first part of this chapter considers future biometrics, with a focus on second generation biometrics that measure physiological patterns. The second discusses the potential biometric future – how the use of biometrics, data and algorithms more broadly, could be used by governments to regulate social and economic interactions. This discussion will draw on the development of credit systems, from those used in commercial online platforms to rate the performance of providers and users, to the more integrated and all-encompassing social credit system (SCS) implemented in China, as an example of a potential future development in liberal democratic countries. Finally, we discuss the key features of liberal democratic theory and how biometric and related technological developments may change governance in western democracies. While we briefly mention some relevant developments in the private sector, our main focus will be on the relationship between liberal democratic governments and their security agencies, on the one hand, and their citizenry, on the other. We describe in general terms how liberal democracies might respond to these new technologies in a manner that preserves their benefits without unduly compromising established liberal democratic institutions, principles and values. Accordingly, we seek to offer a response to some of the dual use ethical dilemmas posed by biometrics, albeit in general terms.

Keywords Biometric identification · Future biometrics · Governance · Digital identity · Social credit system (SCS) · Liberal democracy

5.1 Future Biometrics

There are a range of new biometrics being developed and implemented that provide insights into how biometric technology may influence society in the future. The main biometric identification techniques considered throughout this book – fingerprint, DNA and facial image identification – are examples of first generation biometrics, derived from physical traits. Second generation biometrics, also referred to as behavioural biometrics, measure individual patterns of physiological processes or learned behaviour, rather than physical traits (Smith et al., 2018). These

M. Smith, S. Miller, *Biometric Identification, Law and Ethics*, SpringerBriefs in Ethics, https://doi.org/10.1007/978-3-030-90256-8_5

biometrics are less stable and accurate than first generation biometrics and for that reason are not usually used individually, and have not been widely adopted. Examples include cardiac activity (patterns of heart activity), cognitive biometrics (patterns of brain activity) and gait (pattern of walking). Over time, they are likely to have their own specialised applications, and a role in combination with first generation biometrics to increase accuracy. For example, when integrating facial recognition with CCTV footage to identify individuals in a crowd, distance and lighting conditions affect its accuracy – this can be mitigated through the addition of gait analysis. In relation to access to a computer, fingerprint biometrics could be used as an initial password, and keystroke dynamics to monitor that the same individual is continuing to use the device over time. Cognitive biometrics could be used as a second line biometric in a highly secure environment where it is possible that a fingerprint, or other initial method of access, has been replicated (Smith et al., 2018).

The most recently reported second generation biometric is the remote detection of individual cardiac patterns. The United States military has reportedly developed an infrared laser biometric scanner that can detect unique cardiac signatures, through a person's clothes, from hundreds of meters away, and possibly at even further distances. The technique is described as cardiac laser vibrometry and detects surface movements created by a person's unique heartbeat pattern (Smith et al., 2018). One of the key advantages of the technique is that it provides more accurate results than facial recognition, the other biometric application that can be administered from a distance, and is not affected by factors such as light conditions and headwear (Hambling, 2019). The technology could also be used in the private sector as an alternative to fingerprint identification in the future.

A similar technique which has been established for some time, although cannot be administered at a distance, is cognitive biometric identification. This is based on the measurement of electrical signals that are generated in the brain as a result of an individual's thought processes (Revett et al., 2010). These electrical signals generated by neural activity are representative of individuals' mental states and can be measured by brain-computer interfaces known as electroencephalograms (EEG) (Jolfaei et al., 2013). The measurement of cognitive biometrics is a more invasive process that requires electrodes be placed on the subject's scalp – although a more discrete version may become available as the technology develops. It has been demonstrated that electrical signals in the brain are associated with specific stimuli, and that simply thinking of a specific object or password will create a corresponding electrical pattern that is sufficient for authentication via EEG (Armstrong et al., 2015). However, the technique currently has a lower accuracy than other methods, reportedly ranging from 82% to 97% (Bajwa & Dantu, 2016). Another limitation is the invasive process and high cost of the equipment. While technology generally becomes smaller and cheaper over time, cognitive biometrics are unlikely to be used as widely as the main forms of biometrics that have been discussed.

Another important second generation for of biometric identification is gait recognition. This measures the pattern of motion made by an individual's limbs when they walk (Goffredo et al., 2010). It requires an initial setup stage, to establish an individual's gait. A video recording is converted into a representative silhouette and

data, such as an individuals' height, limb length and torso shape is recorded (Indumathi & Pushparani, 2016). Environmental conditions such as lighting, distance from the camera, and the type of clothing worn by the subject, can affect its use. It has an accuracy rate of approximately 90%, and as discussed, its main application is in conjunction with facial recognition, as it can be operated from a distance, doesn't require as high resolution images, and can function when the subject's face is obscured (Chaurasia et al., 2015).

The final developing form of biometric identification we will consider is keystroke dynamics. This uses an individual's typing characteristics and patterns, such as key press duration, for identification purposes. It is less reliable than physical biometrics due to the variability in behaviour, but its reliability is related to the length of text typed, (e.g., it would have limited application for short passwords) (Rudrapal et al., 2014). The use of keystroke dynamics could increase in the future as part of dual factor authentication in online environments, however broader adoption will be dependent on the availability keyboards, keypads and smartphone screens with pressure sensors that can be integrated with the technology (Ngugi et al., 2012).

Continued technology advancement will lead to a range of more advanced new biometrics being developed in the future; and existing biometrics will become increasing sophisticated and applied in new ways. However, it is the coordinated use of biometrics and big data by governments and corporations that will have the biggest impact on society in the future. In the absence of public debate and law reform to regulate their use, there is potential for these to be used in a way that alters the nature of liberal democracies as they exist today – this will be the focus of the remainder of the chapter.

5.2 Biometric Futures

5.2.1 Social Credit Systems

Developments taking place today in China provide a picture of the direction liberal democracies may shift in the decades ahead as biometric databases and other datasets become more widely available and are used more extensively. The SCS has been developing over the past 20 years and is continuing to advance towards a future society where each citizen is allocated a score representing their honesty and integrity (Sıthigh & Siems, 2019). That score will dictate their lifestyle and access to government and commercial services, including whether a bank will give them a credit card or loan; whether they can travel on public transport; and the schools their children can attend. While this concept is used in specific contexts in liberal democracies, such as in credit scores calculated by lenders, or to rate the integrity of sellers and buyers in online marketplaces, these are not as far reaching or comprehensive as the SCS. Instead of being limited to behaviour in a specific domain, such as

meeting financial obligations, or honouring contracts entered into when buying or selling goods, the fully developed SCS will be all-encompassing in dictating personal actions and behaviours (Sıthigh & Siems, 2019).

The impact of the SCS on individuals becomes more significant and divergent from western versions when used for political purposes in an authoritarian state – such as making judgments about an individual's character, and identifying dissidents or those opposed to certain policies of the Chinese Communist Party, and enforcing consequences against individuals that don't comply. To achieve this end, biometric identification, integrating facial recognition with an extensive public CCTV network, DNA identification, and phone metadata; as well as and big data analytics using sources such as financial and medical records, provide the basis for establishing complete surveillance of a population. As technologies like facial recognition and artificial intelligence become even more widely used, the risk increases that personal data and identity will facilitate a more extensive authoritarian algorithmic governance model (Danaher et al., 2017).

The State Council of the People's Republic of China published a planning outline for the construction of a social credit system in 2014. This publication sets out their rationale for implementing the SCS, with the official goal being the 'construction of sincerity in government affairs, commercial sincerity, social sincerity, and judicial credibility', through greater transparency in government policy making (SCPRC, 2014). A variety of social issues relating to trust that the SCS seeks to address, include fraud, counterfeit goods, tax evasion and food contamination. The Chinese government asserts that moving to a credit-based economy reduces transaction and government intervention in the market, while increasing the country's competitiveness in the global economy. The Chinese government describes three aspects of the SCS. First, the creation of a large interconnected dataset, drawing on the holdings of government and non-government entities, creating: 'Interconnection and interactivity of…credit information systems and…networks that cover all information subjects, all credit information categories, and all regions nationwide' (SCPRC, 2014). This includes data from individuals, businesses, NGOs and government agencies. Second, the application of that data to encourage individuals and organisations to be more trustworthy by preventing those that commit transgressions from accessing services. This operates in the same way that committing traffic offences can lead to a loss of licence; a criminal record can limit employment prospects; or a poor credit rating can make it difficult to obtain a loan from a bank. While some aspects are similar to existing measures in liberal democracies, the SCS is more extensive, implementing automated law enforcement and economic regulation across all aspects of society. Individuals rated as untrustworthy in one aspect of their life may not be able to access services, such as obtaining tickets for flights or high speed rail travel, booking hotel rooms, or accessing the internet. Aside from the inherent rights violations, notably violations of privacy and autonomy, involved in this degree of state interference in the lives of individual citizens, it can also lead to what has been described as a form of informational injustice (van den Hoven, 2008), where information provided in one context can change its meaning when used in another way that leads to disadvantage or discrimination for an individual.

The final aspect is the publication of data to warn members of the public about transacting with untrustworthy individuals and shaming them to alter their behaviour. While details of criminal trials are published in the media in most countries around the world, some Chinese cities have been shaming offenders of minor crimes, such as jaywalking – identifying them using facial recognition technology and posting their image on large public video screens. It has been reported that in cities such as Shenzhen, Jinan and Fuzhou, facial recognition technology has been used to identify offenders who have committed minor crimes such as jaywalking or taking toilet paper from public toilets, and publish their names and pictures on billboards or in the media. Galič et al. (2017) relevantly describes the SCS as '…a tool for assimilating biopower into digital systems' monitoring the faces and movements of bodies in physical spaces as digital representations of individuals.

Many of these measures are extensions or adapted forms of approaches undertaken around the world, and there could be efficiencies and benefits of applying data and technologies such as biometrics to these ends: 'A well-governed SCS could bring transparency, oversee those in power, regulate the economy with less direct government intervention, and encourage people to treat each other more fairly, as the government maintains' (Wong & Dobson, 2019, p. 224). However, there are more concerning aspects that have already begun to be implemented, such as those relating to free speech. Chinese social media sites that allow users to post online commentary are required to maintain lists of those that make statements considered illegal, which can then be integrated in the broader SCS:

> …based on China's record of regulating political speech and other activities, there is no doubt that it could also be abused for social control, prying into every aspect of Chinese citizens' lives and automatically punishing those who don't toe the party line. As in the West, which is awakening to uses and abuses of privately collected data, China's experiment raises moral and economic questions about collection and use of data, which are at the core of the most promising innovations and critical governance challenges worldwide (Chorzempa et al., 2018).

There are parallels between the SCS and the rating systems used in online platforms such as Uber or Airbnb, and the ratings or likes on social media platforms such as Facebook and Instagram (Dahlberg, 2015; Sıthigh & Siems, 2019). These systems quantify individual reputations – those who have higher ratings promoted by the platforms algorithms – and great volumes of data are collected about users and applied for advertising purposes. However, in noting the parallels here, there is a key difference between the SCS which is established and implemented to achieve a political objective, and the use of rating systems in online platforms such as Uber, which are implemented to ensure their platform runs effectively– ultimately a commercial objective. While social media images, posts or metadata is of interest to the governments, particularly in the context of a law enforcement investigation to identify where a person of interest has been, what they have done, or who they have communicated with; the fact that an individual is a courteous Uber driver or passenger, or guest of an Airbnb, is of little interest to government.

On the other hand, there are some parallels between SCS, governments and security agencies in liberal democracies and corporations in respect of control of

personal data including, potentially biometric data. As we have seen, liberal democratic governments and their security agencies have established significant such databases (and employed associated analytics). However, technology corporations, such as Facebook and Google, have adopted a business model according to which individuals provide their personal data in return for 'free' use of internet services. technology corporations. These corporations have been collecting very large amounts of data from their users, e.g. those who conduct searches on Google and those who communicate with their friends on Facebook, and doing so without their knowledge, let alone consent or, at the very least, without their consent until the recent enactment of the European Union's General Data Protection Regulation 2016/679 (GDPR) (although the GDPR only covers the EU and those who interact with the EU). Importantly, these corporations continue to collect very large amounts of data from their users without the *strong* consent of these users (see Chap. 1). Accordingly, this bulk data (or, at least a good deal of it, depending on which particular kind(s) and extent of data, is in question) has been collected in violation of the privacy/data control rights of users of Google and Facebook services. Moreover, data analytics, e.g. machine learning, has been deployed to structure this data in a manner suitable for commercial purposes, notably advertising purposes, e.g. profiles of customers are developed to enable better targeted and, therefore, more efficient and effective, advertisements. The corporations using this data for commercial purposes include not only the corporations who originally collected the data, but also the myriad of other corporations who, as it turns out, they on-sell the data to. Further, according to Zuboff (2019), these commercial activities are not simply to be understood as violations of privacy/data control rights or, as she puts it, the extraction of 'behavioral surplus'. For the quantum of data in question, and the power of the data analytics used, is such as to enable the creation of 'predictive products'. For instance, a bank might construct a new financial product based on far more accurate profiles of bank customers than their use of the bank's existing products. Thus: 'one recent study used the mobility data generated by 100,000 bank customers' cell phones over a one-year period to predict with very high accuracy their likely demand for a given loan product.'[1] Given this predictive ability and the ability to use manipulative techniques, e.g. subliminal advertising and the use of so-called 'nudges' (Thaler & Sunstein, 2009), the possibility of 'behavioral modification' emerges, although Zuboff herself emphasizes the predictive ability as opposed to what we take to be the conceptually separable manipulative techniques. Of course, the power of manipulative techniques is enormously enhanced by predictive ability. At any rate, important questions now arise in relation to biometric data collected and stored by corporations. The discussion of Clearview AI in Chap. 3 is a case in point.

[1] Mariano-Florentino Cuéllar and Aziz Z. Huq review of Zuboff's Age of Surveillance Capitalism in *Harvard Law Review* vol. 133 2020 note 51 p. 1291) who reference in turn Cagan Urkup et al., Customer Mobility Signatures and Financial Indicators as Predictors in Product Recommendation, 13 PLOS ONE, July 2018, at 1, 2–5.

Social media is also analysed by law enforcement in liberal democracies. Predictive policing applies analytical techniques to identify likely targets in police investigations and allocate resources, including deriving intelligence from platforms such as Facebook and Instagram (Binder, 2016). As was discussed in Chap. 2, the use of social media in investigating the attack on the Capitol Building in January 2021 indicates how valuable it can be as a resource for law enforcement agencies. This is in spite of the fact that it is now well publicised since 2013 that law enforcement and security agencies are using social media resources extensively in their investigations and intelligence activities. The Snowden revelations provided evidence of a propensity for Western intelligence services to use this data on both individual and societal levels where it is relevant to their targets:

> The concept of surveillance is not unfamiliar in democratic states. The United States, The United Kingdom, and Australia are, for instance, continuously implementing additional surveillance infrastructures and legislatures, at the same time as prominent debates continue about citizen's privacy and rights in relation to their individual data… China's social credit system should be viewed as a warning to Western liberal democratic countries of what may be to come. As our technological age allows for vast amount of data to be collected from individuals across multiple platforms, integrated and used to construct representational profiles and map patterns and behaviours, as well as the continuous rating of others via rating applications, the digitising of identity and reputation is already well underway (Wang & Dobson, 2019, p. 228).

The biometric identification and data integration capabilities being utilised by China in the SCS are all available in liberal democracies, and are currently being used in a less systematic way. To date, China is the only country to have centralised and formalised a system that seeks to determine the value of an individual in a country and regulate their behaviour accordingly, using these capabilities; however, there is certainly the potential for this to occur in an incremental manner in countries around the world if steps are not taken to regulate these technologies more proactively with a view to preventing similar systems from being implemented gradually.

5.2.2 Technology-Based Regulation

Biometric technology is steadily becoming the main form of digital identity. Digital identity is vital to transacting in the online environment, where the majority of transactions will soon take place. As technology advances, the regulation of transactions through the use of technical system architecture is becoming an increasingly important addition to regulation using legislation and common law. Blockchain is a form of distributed ledger technology, with Bitcoin being the best known to date. Bitcoin facilitates peer-to-peer transactions, without the need for bank processing, using blockchain technology to record transactions and ownership. Bitcoin transactions are verified by other users of the network (Australian Government, 2020). Smart contracts are a more recent development of blockchain technology that enable legal contracts to be automatically executed by code to implement an agreement

between parties, rather than being drafted on paper by a lawyer. Peer-to-peer networks validate conditions that initiate the automated execution of the contract. Rather than the contract being enforced by a court, the code written into the block chain guarantees the performance of the agreement (Governatori et al., 2018). Smart contracts prevent transactions taking place until a condition or threshold has been digitally validated, such as funds being transferred into an account. By contrast, traditionally hardcopy documents were signed as a means of verifying identity and signifying agreement. If a dispute occurred, legal recourse followed through the court system after a breach, and even then, would regularly be a matter of dispute, requiring significant amounts of time and money to be spent on legal representation in order to enforce it. Smart contracts therefore use technology to proactively prevent parties taking actions that are outside the terms of the contract–they are however, only as good as the data they rely upon.

Biometric identification is a means of validating identity that integrates effectively with these approach in an online environment, and will become increasingly used in this context. While a feature of bitcoin and blockchain to date is that they have bypassed government regulated sectors, such as banking and the legal profession, over time government infrastructure will likely be introduced to facilitate these transactions, and when that occurs, the government may have more, rather than less, control.

Regulatory theorists such as Joel Reidenberg and Lawrence Lessig have described the use of system architecture itself as an approach to regulation. Reidenberg uses the phrase *Lex Informatica* to refer to 'law' imposed by technological capabilities and system designs, rather than by legally proscribing activities by legislation:

> …law and government regulation are not the only source of rule-making. Technological capabilities and system design choices impose rules on participants. The creation and implementation of information policy are embedded in network designs and standards as well as in system configurations…the set of rules for information flows imposed by technology and communication networks form a *Lex Informatica* that policymakers must understand, consciously recognize, and encourage (Reidenberg, 1998, p. 553).

Lessig describes the interaction of system architecture with three other modalities: black letter law, social norms and market forces (Lessig, 1999; Miller, 2010). Regulators can use combinations of these to control activities, in both the real and digital contexts. For instance, law controls individual activities through the threat of legal sanctions, such as fines or imprisonment; supported by the market through pricing; stigma associated with illegal behaviour; and computer system architecture, such as a requirement that internet service providers block illegal websites. Acknowledging that online and digital environments are difficult to regulate–a regulatory framework, combining law with other modes, is necessary to be effective.

One advantage of system architecture based regulation is the high level of compliance, as circumvention usually requires advanced technical skills, can be efficient to implement because the private sector can be required to develop the infrastructure, and it does not take as long as enacting laws through parliament (although this raises questions of political accountability) (Lessig, 1999). Governments around the world are beginning to use these forms of regulation for

new technologies such as blockchain and smart contracts that provide insights into the role that biometrics, big data, and algorithm-based decision making may have in the commercial sector in the future. It seems clear that biometrics will likely have an increasingly important role in identifying people transacting in online environments.

The establishment of system architecture to regulate smart contracts and digital currencies will provide the foundation for blockchain to become a mainstream part of the financial system in the future, providing authentication, security and auditability for digital currency transactions, and throughout the lifecycle of smart contracts. In late 2019, China announced it would launch its own cryptocurrency and associated infrastructure, setting out a timeline for this to take place over the years ahead (Cuthbertson, 2019). Western democracies, such as Australia are introducing similar approaches. A consortium between the government and private sector has begun work to establish an Australian National Blockchain (ANB) to enable businesses to digitally manage contracts, exchange information and conduct authentication:

> The ANB will allow organisations to digitally manage the lifecycle of a contract, not just from negotiation to signing but also continuing over the term of the agreement, with transparency and permissioned-based access among all parties in the network, by using blockchain-based smart contracts to trigger business processes and events. These contracts contain smart clauses which have the ability to record external data sources, such as Internet of Things (IoT) device data and self-execute if specified contract conditions are met (ANB, 2020).

Biometric identification can play an important role in the verification and security of online transactions involving smart contracts and bitcoin. It is likely that as biometrics becomes more widely used as an identifier, governments will need to provide central systems for the protection and verification of biometric profiles, rather than have them continue to be held in the various databases of private companies. In the same way that governments have seen the need to maintain infrastructure relating to smart contracts and bitcoin, in order for the commercial sector to have confidence in the technology, it is likely that will they will also recognise this need in relation to biometrics, as they become a proxy for identity in online transactions. In the light of concerns about corporations' misuse of personal data in general, and about the inability of governments effectively regulate technology corporations, this increased role of government would be welcome developments. However, it does now raise questions with respect to citizens' rights to their biometric data vis-à-vis governments. Part of the response to these questions might be the establishment of public sector organisations with relevant legislated authority over the storage and access to biometric data, e.g. statutory authorities, which are independent of both the private sector and governments.

5.3 Liberal Democracy

At various points in the discussions of biometric technology in this work we have invoked liberal democratic values, e.g. individual privacy/autonomy, and principles, e.g. freedom from interference from government if one has not committed a crime and is not reasonably suspected of having committed one, and done so in part because of the threat posed to liberal democratic values by biometric technology and big data, or, at least, certain uses of it (Miller, 2021; Miller & Bossomaier, 2021; Miller & Gordon, 2014). Moreover, we have provided ethical analyses of the uses for security purposes of particular biometric technologies, notably fingerprinting, facial recognition technology and DNA. Moreover, in the last chapter we discussed the integration of these technologies with non-biometric technologies. While space did not permit a comprehensive ethical treatment of these issues we did suggest that the problems needed to be framed, firstly, in terms of individual rights versus collective goods (Miller, 2010 Ch. 2) and, secondly, in terms of dual use dilemmas (Miller, 2018), i.e. roughly speaking, dilemmas arising because the use of these technologies has the potential to confer great benefits but also to impose great moral costs. In doing so we noted that the dual uses in question cut across the individual rights versus collective goods distinction since some of the uses of the technologies potentially benefited individual rights (e.g. right to personal security) and undermined collective goods (e.g. collective power of the citizenry in relation to the state). As we have just seen there is an emerging suite of second generation biometrics, e.g. gait analysis, cardiac activity. Each of these technologies and corresponding uses is in need of ethical analysis. However, as we have also just seen, while there is at this point in time inadequate ethically informed direction being given in relation to first generation and, more obviously, second generation biometrics, let alone the integration of biometric technologies with non-biometric technologies, there is one possible direction increasingly on display, namely, China's use of integrated biometric and non-biometric technologies to enable the realisation of its social credit system and, ultimately, to underpin an authoritarian state. There is also an increasing and somewhat alarming power imbalance within liberal democracies between technology corporations and individual citizens, and an accompanying inability of liberal democratic governments to address this imbalance.

The direction in which China is going is profoundly at odds with liberal democratic values and principles; indeed, it is entirely inconsistent with both of the pillars of liberal democracy, i.e. liberalism and democracy. Liberalism is committed to individual autonomy, i.e. freedoms of thought, speech, movement, assembly, etc., and entails significant limits on state power; democracy is committed to universal rights to vote and hold office, multiple political parties, free and fair elections, etc., and is inconsistent with an authoritarian state since in essence democracy entails government of the people, *by the people,* for the people. Moreover, liberal democracies seek to limit and dilute the power of the state by an assemblage of interrelated institutional arrangements and associated principles, including constitutions, the rule of law (as opposed to the rule of 'men'), separation of powers, (executive,

legislature, judiciary), free and independent press, a free market and private ownership, including private ownership or, at least control, of personal data and, therefore, biometric data. Authoritarian states lack all or most of these institutional arrangements, or have them in name only or only to a limited degree.

That said, the contrast between contemporary liberal democracies, e.g. US, and some contemporary authoritarian states, e.g. Russia, should not be overstated. This is in part because there is at least one important feature of contemporary liberal democratic states which is evidently inconsistent with liberal democratic principles and, in particular, the autonomy of individual human beings, namely, powerful, hierarchically structured, private sector organisation, e.g. notably multinational corporations. Typically, most of the employees in these organisations have very little control over their actions qua employees which is to say over much of the activity they undertake during the course of their lives. In addition, as mentioned in earlier chapters, the customers of some of the largest of these corporations, e.g. the big tech companies such as Facebook and Apple, are subject to manipulation of a kind that compromises their autonomy, e.g. as a result of a business model according to which customers provide their personal data in return for the services provided rather than paying for them. More generally, private companies are by one means or another acquiring biometric data and using biometric technologies, e.g. Clearview's acquisition of billions of facial images scraped off the Internet and employment of facial recognition technology. We have argued that there can be adequate moral justifications for security agencies in liberal democratic states to use biometric technologies to provide the collective good of security if the use of these technologies is, for instance, necessary and proportionate, and if appropriate accountability mechanisms are in place. However, the use of biometric technologies by private companies for profit is an entirely different matter. Arguably, the use of facial recognition technology by private companies for profit, as in the case of Clearview, should simply be banned. In addition, speaking generally, biometric data should not be controlled by corporations; other more desirable institutional arrangements are possible such as, as mentioned above, storage of such data in organisations independent of corporations (and of governments and security agencies), e.g. statutory authorities. Here we need to distinguish between ownership of biometric data, storage of biometric data and access to biometric data. Depending on the biometric data in question, arguably, individual citizens should retain (defeasible) ownership rights over their biometric data, the independent authorities' should be granted storage rights in respect of this data (under restricted conditions) and security agencies granted rights of access to it (under warrant).

But to return to our larger canvas, China's social credit system conveniently illustrates a fundamental difference between liberal democracies and authoritarian states. The underlying assumptions of the social credit system are that the state ought to, firstly, determine what the collective good(s) of the citizenry are (in part, of course, by recourse to the uncontroversial de facto needs, such as food, clothing and shelter, of the citizens); secondly, determine what counts as being a good citizen, (e.g. someone who contributes to those collective goods but, in addition, who accepts the authority of the authoritarian state and complies with its laws,

regulations and policies); and, thirdly, ensure that the citizens behave accordingly. In relation to the compliance of its citizens, China's embrace of biometric technology integrated with non-biometric technologies, has a crucial role to play (as described above). While liberal democratic states will inevitably embrace new and emerging technologies, including biometric technology, and the benefits they confer they must do so on their own terms, i.e. in a manner that does not undermine liberal democracy. By contrast with this authoritarian conception of the state, the liberal democratic state is not, or ought not to be, in the business of determining what are or are not the collective goods to be provided or what counts as a good citizen, and ensuring compliance with this model. Indeed, the reverse is the case; the citizenry ought to decide about these questions of collective goods and the state ought to enact its laws and frame its policies accordingly. Appropriately regulated, new and emerging technologies, such as social media, can facilitate liberal democracies by, for example, enabling large numbers of citizens to communicate with one another and leaders to communicate directly with citizens. Identification technologies, including biometrics, may well have a role to play here by, for example, ensuring that communicators are able to be identified and held accountable by those who they communicate with.

Moreover, if the government of the day fails to adequately represent its citizens or otherwise serve their collective interests, then, the members of the citizenry have the collective right (i.e. joint right (Miller, 2010 Ch. 2) – see Chap. 3 for discussion) to replace it via an election. Again, identification technologies, including biometrics, may have a role to play in relation to authenticating voters. And there is a further important point regarding the relationship of the individual to his or her fellow citizens in liberal democratic states.

Importantly, the rights of the individual (and of minorities) need to be protected from the tyranny of the majority and, more generally, from predatory groups. Here constitutions, such as the US constitution, have an important role to play, e.g. the right to free speech, as have law enforcement agencies impartially enforcing the law. In so far as new and emerging technologies, including biometrics, assist law enforcement agencies to impartially enforce laws that protect moral rights, these technologies should be embraced, as they largely have been, e.g. improved methods of fingerprinting and DNA.

However, in relation to the protection of the rights of the individual (and of minorities), including from the state and from the tyranny of the majority, the notion of freely undertaken joint action also has an important role to play, although this might at first seem counter-intuitive. Firstly, consider freedom of assembly, free and fair elections, and the moral rights to engage in these activities. These phenomena involve, we suggest, individuals freely undertaking *joint* action (Miller, 2010) (see Chap. 1 for discussion); one cannot participate in an assembly or an election on one's own. Moreover, and relatedly, these joint actions involve these individual freely exercising their joint rights (Miller, 2010 Ch. 2) (see Chap. 3 for discussion).

The enjoyment of rights is typically thought to be an individual affair; and indeed in many respects it is. If, for example, a person, A, has a right to individual freedom

and it is fulfilled, then A enjoys the exercise of A's right and no-one else enjoys the exercise of A's right (even if, B for instance, enjoys the exercise of B's right). It is also true that the exercise of A's right to freedom is logically consistent with the inability of others to exercise their respective rights to freedom, e.g. if A is Robinson Crusoe living alone on an island cut off from civilisation and everyone else, i.e. B, C, D etc., lives in an authoritarian state.

It is a commonplace of political philosophy that the establishment of government and the rule of law is *instrumentally* necessary for the preservation of the freedom of each of us, albeit under the restriction not unduly to interfere with others; the alternative, as Hobbes famously said, is the state of nature in which life is nasty, brutish and short. However, we want to make a somewhat different point; there is another reason that most of us rely on the fulfilment of the rights to freedom of others in order to enjoy adequately our own freedom.

Specifically, person A cannot engage in (freely performed) *joint* activity with others, if these others cannot exercise their rights to freedom (Miller, 2010 Ch. 3). For example, A cannot freely participate in elections, unless others can also do so; hence the absurdity of A voting in an election in which all the other votes were cast in accordance with the instructions of the dictator of the country in question.

Indeed, joint action is (in part) constitutive of all institutions, political, economic and otherwise (Miller, 2010). Accordingly, unless A is the one, or one of the ones, who is in control of the actions of others – including determining their participation in joint activity – then A's freedom is (literally, and not merely figuratively) diminished to the extent that the freedom of others is. So the fulfilment of one person's right to freedom is importantly connected, directly or indirectly – via a pervasive network of joint institutional activity – to the fulfilment of the rights to freedom of many other persons. So the right to freedom of action, including freedom of assembly and freedom to vote in free and fair elections, are in part *joint rights* to engage in freely performed *joint action* (Miller, 2010 Chs. 2 & 3). Accordingly, to the extent that new and emerging technologies, such as social media, blockchain, identification technologies, and so on facilitate the exercise of joint rights to engage in joint activity that serves the collective ends of legitimate institutions, whether they be democratic governments, institutions of public communication, law enforcement agencies or financial institutions, then these technologies benefit rather than undermine liberal democracies.

5.4 Conclusion

As we saw in our discussions in previous chapters of existing biometrics and, especially, biometric and non-biometric integration, biometrics poses a series of dual use ethical dilemmas for liberal democracies. The same point holds even more in relation to future developments: biometrics has the potential to provide enormous benefits but also to cause great harm.

There are two aspects of future developments in relation to biometric identification that need to be considered. The first is new biometric technologies using unique physiological processes such as brain waves and cardiac rhythms that could provide greater accuracy and be more difficult to replicate. The second is the way that biometric data will change the governance of societies as it becomes the primary means of identity verification. The significance of the general points concerning joint action and joint rights in relation to political participation, and the potential facilitating roles of new and emerging technologies we have raised above, including to freely assemble and engage in free and fair elections, is as follows. Firstly, that the sharp contrast sometimes drawn between the two core components of liberal democracy, namely liberalism and democracy, is overdrawn. Properly understood, democracy is an expression of individual freedom, namely, freely undertaken joint action and, as such, stands in sharp contrast with authoritarianism.

Secondly, and relatedly, the sharp contrast that might be drawn between individual rights to freedom (e.g. privacy/autonomy) and collective goods facilitated by biometric identification (e.g. security) is overdrawn. For, at least in principle, citizens in a liberal democracy can freely (jointly) choose (directly or via their representatives) uses of biometric technologies that facilitate the collective good of security (and do so in a manner, at least in theory, consistent with preserving basic privacy rights, for example). If so, their rights to freedom are, at least to this extent, exercised rather than compromised. Naturally, if they make bad choices in this regard and, for instance, allocate too much surveillance power to the state and, thereby, jointly choose slavery (so to speak), then their individual rights to privacy/autonomy will be compromised – and perhaps also, via the increased power of the state, their freedoms in general. But this is far from inevitable; rather the collective (i.e. joint) decision is theirs to make.

Thirdly, liberal democracies commitment to individual autonomy and, as we are suggesting, the related value of freely chosen joint action, implies that reliance on widespread compliance with freely accepted, rationally-based, moral principles (e.g. principles of fairness) reinforced by social approval/disapproval, i.e. reliance on socio-moral norms, is to be preferred to reliance on compliance with top-down laws and regulations based on fear of punitive formal sanctions (such as the Social Credit System). Here we stress the freely accepted, rationally-based, moral dimension of the socio-moral norms in question, and also the fact that they are bottom-up. We note that new and emerging technologies can reinforce or undermine socio-moral norms; as mentioned above, it depends on how the technology is used, and by whom for what purpose. By contrast, authoritarian states prefer to rely on top-down laws and regulations based on fear of punitive sanctions and applied by authorities in the context of a state characterised by widespread use of surveillance technology and a docile, fearful population all too willing to report the 'transgressions' of fellow citizens to authorities. Importantly, for our purposes here and as we have seen, in contemporary authoritarian states the surveillance technology in question increasingly consists of biometrics technology integrated with non-biometric technologies such as smartphone metadata.

Fourthly, and relatedly, whether liberal democratic states retain their liberal-democratic character in the face of these technological and related developments depends on a number of factors. These include: (i) clear articulation and legal enshrinement of individual ownership rights to biometric data – including joint ownership rights in the case of genomic data – as distinct from the storage and access rights of governments, security agencies, statutory authorities and private sector organisations; (ii) clear articulation of, and compliance of governments, legislation and security agencies with, constitutive liberal democratic principles as they relate to biometric and other forms of identification technology, e.g. clear and significant limits on infringements of individual rights to privacy/autonomy, application of principles of necessity and proportionality to uses of new technologies, law enforcement accountability measures (e.g. use of judicial warrants), democratic accountability of governments, security agencies, laws, regulations and policies, e.g. via elected representatives and parliamentary committees but also privacy commissioners etc.; (iii) well-functioning, independent, epistemic (i.e. knowledge-based) institutions, e.g. statutory authorities to store biometric data, news media, universities (Miller, 2020); (iv) well-informed, rational and engaged citizenry (and the utilisation of well-regulated new and emerging technologies to achieve this); (v) an ability to embrace new and emerging technologies, such as biometric identification, in the service of individual and joint moral rights and liberal democratic institutions.

References

Armstrong, B., Ruiz-Blondet, M., Kahalifian, N., Kurtz, K., Jun, Z., & Laszlo, S. (2015). Brainprint: Assessing the uniqueness, collectability, and permanence of a novel method for ERP biometrics. *Neurocomputing, 166*, 59–67.

Australian Government. (2020). *National blockchain roadmap*. Department of Industry, Science, Energy and Resources.

Australian National Blockchain (ANB). (2020). *A new digital backbone for business.* https://www.australiannationalblockchain.com/

Bajwa, G., & Dantu, R. (2016). Neurokey: Towards a new paradigm of concealable biometrics-based key generation using electroencephalograms. *Computers and Security, 62*, 95–113.

Binder, C. (2016). Happenings foreseen: Social media and the predictive policing of riots. *Security and Peace, 34*, 242–247.

Chaurasia, P., Yogarajah, P., Condell, J., Prasad, G., McIlhatton, D., & Monaghan, R. (2015). Biometrics and counter-terrorism: The case of gait recognition. *Behavioural Sciences of Terrorism and Political Aggression, 7*, 210–226.

Chorzempa, M., Triolo, P., & Sacks, S. (2018). China's social credit system: A mark of progress or a threat to privacy? *Peterson Institute for International Economics Policy Brief 18-14*.

Cuthbertson, A. (2019, 30 October). China bans anti-blockchain sentiment as it prepares for launch of state cryptocurrency. *The Independent*. https://www.independent.co.uk/life-style/gadgets-and-tech/news/china-cryptocurrency-blockchain-bitcoin-a9176636.html

Dahlberg, L. (2015). Expanding digital divides research: A critical political economy of social media. *Communication Review, 18*, 271–293.

Danaher, J., et al. (2017). Algorithmic governance: Developing a research agenda through the power of collective intelligence. *Big Data & Society*, *July–December*, 1–21.

Galič, M., Timan, T., & Koops, B. J. (2017). Bentham, Deleuze and beyond: An overview of surveillance theories from the panopticon to participation. *Philosophy & Technology, 30*, 9–37.

Goffredo, M., Bouchrika, I., Carter, J., & Nixon, M. (2010). Performance analysis for automated gait extraction and recognition in multi-camera surveillance. *Multimedia Tools and Applications, 50*, 75–94.

Governatori, G., et al. (2018). On legal contracts, imperative and declarative smart contracts, and blockchain systems. *Artificial Intelligence and Law, 26*, 377–409.

Hambling, D. (2019, 27 June). The Pentagon has a laser that can identify people from a distance – By their heartbeat. *MIT Technology Review*. https://www.technologyreview.com/2019/06/27/238884/the-pentagon-has-a-laser-that-can-identify-people-from-a-distanceby-their-heartbeat/

Indumathi, T., & Pushparani, M. (2016). Automatic door opening using gait identification for movement as gesture. *Journal of Engineering Technology, 4*, 132–140.

Jolfaei, A., Wu, X., & Muthukkumarasamy, V. (2013). On the feasibility and performance of pass-thought authentication systems. In K. D. McDonald-Maier, G. Howells, & A. Stoica (Eds.), *IEEE computer society 2013 fourth international conference on emerging security technologies* (pp. 33–38). Conference Publishing Services.

Lessig, L. (1999). *Code and other laws of cyberspace*. Basic Books.

Miller, S. (2010). *The moral foundations of social institutions: A philosophical study*. Cambridge University Press.

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

Ngugi, B., Tarasewich, P., & Reece, M. (2012). Typing biometric keypads: Combining keystroke time and pressure features to improve authentication. *Journal of Organizational and End User Computing, 24*, 42–63.

Reidenberg, J. (1998). Lex informatica: The formulation of information policy rules through technology. *Texas Law Review, 76*, 553–593.

Revett, K., Deravi, F., & Sirlantzis. (2010). Biosignals for user identification: Towards cognitive biometrics? In G. Howells et al. (Eds.), *IEEE computer society 2010 conference on emerging security technologies* (pp. 71–76). Conference Publishing Services.

Rudrapal, D., Das, S., & Debbarma, S. (2014). Improvisation of biometrics authentication and identification through keystroke pattern analysis. In R. Natarajan (Ed.), *Distributed computing and internet technology: 10th international conference* (pp. 287–292). Springer.

Sıthigh, D. M., & Siems, M. (2019). The Chinese social credit system: A model for other countries? *The Modern Law Review, 82*, 1034–1071.

Smith, M., Mann, M., & Urbas, G. (2018). *Biometrics, crime and security*. Routledge.

State Council of the People's Republic of China (SCPRC). (2014, June 14). *Planning outline for the construction of a social credit system* (English translation: Creemer, R.). https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-asocial- credit-system-2014-2020/

Thaler, R., & Sunstein, C. (2009). *Nudge*. Penguin.

van den Hoven, J. (2008). Information technology, privacy and the protection of personal data. In J. van den Hoven & J. Weckert (Eds.), *Information technology and moral philosophy*. Cambridge University Press.

Wong, K., & Dobson, A. (2019). We're just data: Exploring China's social credit system in relation to digital platform ratings cultures in westernised democracies. *Global Media and China, 4*, 220–232.

Zuboff, S. (2019). *The age of surveillance capitalism*. Profile Books.