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.