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.