Introduction

Facial Recognition in the Modern State

Rita Matulionyte and Monika Zalnieriute

I.1 FACIAL RECOGNITION AND ITS CHALLENGES

From border control to policing and welfare, governments are using automated facial recognition technology (FRT) to collect taxes, prevent crime, police cities, and control immigration. 70 per cent of police forces have access to some form of the technology and 60 per cent of countries have facial recognition in some airports.[1] In Australia, France, the United Kingdom, Germany, the Netherlands and the United States, it has been employed by border security at the arrival gates.[2] It has been used or trialled in national policing efforts to detect suspects or missing people in various countries.[3] FRT is increasingly used by governments for identity verification and identification, as well as categorisation or counting.

Concerns around an increased use of automated FRT, especially in public spaces such as airports, train stations, and city streets, have been expressed across the globe. Privacy and data protection, bias and discrimination, the lack of transparency, explainability, public oversight, and accountability are among the most popular concerns associated with FRT. Freedom of expression, peaceful association, and assembly are other examples of the fundamental rights that can be impacted and undermined by

[1] Paul Bischoff, 'Facial recognition technology (FRT): 100 countries analyzed' (8 June 2021), Comparitech, www.comparitech.com/blog/vpn-privacy/facial-recognition-statistics/#:~:text=Five%20countries.

[2] Ibid.

[3] Australia: E. Gillespie, 'Are you being scanned? How facial recognition technology follows you, even as you shop' (4 March 2019), *The Guardian*, www.theguardian.com/technology/2019/feb/24/are-you-being-scanned-how-facial-recognition-technology-follows-you-even-as-you-shop; Canada: Office of the Privacy Commissioner of Canada (OPC), 'Police use of facial recognition technology in Canada and the way forward' (10 June 2021), www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/; Italy: European Digital Rights (EDRi), 'Italy introduces a moratorium on video surveillance systems that use facial recognition' (15 December 2021), https://edri.org/our-work/italy-introduces-a-moratorium-on-video-surveillance-systems-that-use-facial-recognition/; France: Statewatch, 'Legal action against police facial recognition technology' (22 September 2020), www.statewatch.org/news/2020/september/france-legal-action-against-police-facial-recognition-technology/; United Kingdom: Rhiannon Williams, 'UK police forces testing new retrospective facial recognition that could identify criminals' (31 July 2021), *i news*, https://inews.co.uk/news/technology/uk-police-testing-retrospective-facial-recognition-identify-criminals-1128711.

FRT. These risks have been recognised both by courts and policymakers alike. For instance, the UK police use of automated FRT was successfully challenged in 2020 in the *Bridges* case, where the Court of Appeal of England and Wales held that police use of automated FRT was unlawful because it was not 'in accordance with law' under Article 8 of the European Convention of Human Rights.[4]

Ethical and legal risks of FRT have led many non-governmental organisations (NGOs), professional organizations, local municipalities, and legislators around the globe to call for regulation or even outright bans on FRT use. In the United States, FRT use was initially suspended in a number of the states, with some of the temporary bans being recently lifted.[5] In the EU, the draft EU Artificial Intelligence Act suggests that law enforcement could be allowed to use live FRT in certain exceptional scenarios,[6] while the European Parliament has called for an outright ban of certain FRT uses.[7] Recent cases in China to a certain extent limited FRT uses by the private sector,[8] while an extensive employment of FRT by government remains intact. Regional and international organizations, such as the European Data Protection Authority, World Economic Forum, and Interpol developed specific guidelines on how FRT should be used in law enforcement context.[9]

However, regulatory solutions are lagging behind. Owing to the controversy of the technology and multiple competing interests, there is yet no country that has a comprehensive legal framework regulating the use of FRT by states. Policymakers around the world are struggling to find the most suitable regulatory solutions to both enable the beneficial uses of facial recognition and manage threats posed by these technologies.

Academic literature on FRT is expanding, with legal literature mostly focussing on privacy and data protection implications of FRT.[10] Previous books on AI and law in general touch upon some of the issues this book covers, such as transparency, discrimination and privacy issues of AI, however, they lack a specific focus

[4] *R (Bridges)* v. *South Wales Police* [2019] EWHC 2341, High Court; [2020] EWCA Civ 1058, Court of Appeal.

[5] P. Dave, 'U.S. cities are backing off banning facial recognition as crime rises' (13 May 2022), *Reuters*, www.reuters.com/world/us/us-cities-are-backing-off-banning-facial-recognition-crime-rises-2022-05-12/.

[6] European Commission, 'Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative Acts' (2021), COM, 206 Final.

[7] European Parliament, 'Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters' (2021) (Report-A9-0232/2021).

[8] See *Guo Bing v. Hangzhou Safari Park Co*., Ltd., Hangzhou Fuyang District People's Court Case No. (2019) Zhe 0111 Minchu 6971, 20 November 2020.

[9] World Economic Forum, UNICRI, INTERPOL, Netherlands Police, 'A policy framework for responsible limits on facial recognition' (2022); European Data Protection Board (EDPB), 'Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement', version 1 (12 May 2022), https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf.

[10] See, e.g., M. N. Harnois, *Facial Recognition Technology: Best Practices, Future Uses and Privacy Concerns* (Nova Science, 2013); E. J. Kindt, *Privacy and Data Protection Issues of Biometric Application* (Springer, 2013).

on FRT.[11] Books dealing specifically with FRT examine isolated legal issues related to FRT such as privacy and data protection,[12] or legal challenges posed by FRT in specific jurisdictions.[13] Authors in disciplines other than law track technological progress in FRT and detail its uses globally,[14] analyse the technological limitations of these technologies,[15] or its challenges in specific government sectors, such as the criminal justice system.[16] However, there is currently no book in law that offers an international comparative examination of legal challenges and regulatory initiatives targeting FRT in jurisdictions around the globe. FRT raises similar legal and ethical challenges around the world, and thus a global discussion and exchange of lessons learned and best practices are needed to inform national and regional policy discussions and regulation of FRT. Moreover, there is still a lack of interdisciplinary discussions where law, technology, and social and political science academics share and exchange their insights on how to approach challenges posed by facial recognition technologies.

I.2 THE AIM AND ORIGIN OF THIS BOOK

This book aims to provide the first in-depth socio-legal analysis and international comparison of government use of FRT across domestic and regional jurisdictions in five regions of the globe (Europe, North America, South America, Asia-Pacific, and Africa). Building on comparative legal methods, qualitative interviews, political theory, and case studies, the book examines how FRT is increasingly used by different governments, what legal and ethical challenges different FRT uses raise, and whether legal and governance frameworks that have been implemented or proposed by various stakeholders to address these challenges in diverse jurisdictions are adequate and appropriate.

[11] See, e.g., W. Barfield (ed.), *Cambridge Handbook on the Law of Algorithms* (Cambridge University Press, 2021); S. Chesterman, *We, the Robots? Regulating Artificial Intelligence and the Limits of the Law* (Cambridge University Press, 2021); R. Abbott, *The Reasonable Robot: Artificial Intelligence and the Law* (Cambridge University Press, 2020); M. Ebers and S. Navas (eds.), *Algorithms and Law* (Cambridge University Press, 2020); J. De Bruyne and C. Vanleenhove (eds.), *Artificial Intelligence and the Law* (Intersentia, 2021); D. E. Harasimiuk and T. Braun, *Regulating Artificial Intelligence: Binary Ethics and the Law* (Routledge, 2021); J. Turner, *Robot Rules; Regulating Artificial Intelligence* (Springer, 2019).

[12] See Harnois, *Facial Recognition Technology*; Kindt, *Privacy and Data Protection Issues*.

[13] For example, N. Lynch, L. Campbell, J. Purshouse, and M. Betkier, *Facial Recognition Technology in New Zealand: Towards a Legal and Ethical Framework* (Law Foundation New Zealand, 2020); J. Lynch, *Face Off: Law Enforcement Use of Facial Recognition Technology* (published independently, 2019), with a focus on the United States.

[14] K. A. Gates, *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance* (New York University Press, 2011).

[15] S. A. Magnet, *When Biometrics Fail: Gender, Race, and the Technology of Identity* (Duke University Press, 2011).

[16] M. Smith, Monique Mann, and Gregor Urbas, *Biometrics, Crime and Security* (Routledge, 2018). A. G. Ferguson *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (New York University Press, 2017).

The book focusses on FRT use *by government*, which has raised most significant concerns around the globe. Governments are able to use FRT to exert power with coercion, which is not possible for private sector companies. The role of private technology companies and their collaboration with governments when deploying FRT is, however, touched on in many chapters of this collection (e.g., Chapter 7 on protests, Chapter 17 on China), as are legal tools corporations and governments use to shield their collaboration from public eye (Chapter 4 on transparency and trade secrets).

The chapters for this collection are based on the presentations made at an international conference, *Facial Recognition in the Modern State*, held online in September 2022. The conference and this book were a part of the project on *Government Use of Facial Regulation Technologies: Legal Challenges and Possible Solutions (FaceAI)*, funded by the Lithuanian Research Council (2021–2023) and conducted by Rita Matulionyte, Monika Zalnieriute, Agne Limante, and Egle Kavoliunaite-Ragauskiene.

I.3 STRUCTURE OF THE BOOK

The book is structured in two main sections.

Part I, ‘Facial Recognition Technology in Context: Technical and Legal Challenges’, written by experts in technology, law, and sociology, explores the main legal, social, ethical, and technological challenges related to FRT. Five chapters introduce technical FRT aspects and explore socio-legal challenges posed by FRT, especially to the rule of law and to fundamental rights such as a right of information, privacy, non-discrimination, freedom of information, and political freedoms.

Chapter 1, written by a team of researchers in social science – Neil Selwyn, Mark Andrejevic, Chris O’Neil, Xin Gu, and Gavin Smith – provides an introductory overview of the recent emergence of FRTs into everyday societal contexts and settings. It provides valuable social, political, and economic context to the legal, ethical, and regulatory issues that surround this fast-growing area of technology development. The authors argue that despite the seemingly steady acceptance and practical take-up of FRT throughout everyday life, FRT technology still poses significant risks and requires continued critical attention from scholars working in the social, cultural, and legal domains.

Chapter 2, written by a computer scientist and an industry expert in computer vision, Ali Akbari, introduces legal audiences to FRT from a technical perspective. This chapter explains the fundamentals of AI and FRT, their common development life cycle, essential building blocks, and some of the crucial challenges that computer and data scientists currently face in ensuring the accuracy, effectiveness, and trustworthiness of these technologies. This technical introduction will serve as a foundation to the examination of legal and ethical challenges surrounding FRT technologies, which are frequently connected to technical characteristics of the technology.

Cambridge University Press & Assessment
978-1-009-32119-8 — The Cambridge Handbook of Facial Recognition in the Modern State
Edited by Rita Matulionyte, Monika Zalnieriute
Excerpt
More Information

Chapter 3, by Simon Michael Taylor, introduces the reader to FRT history and development of FRT from the perspective of science and technologies studies. Grounded in the history of science and technology, the chapter demonstrates how critical aspects of FRT infrastructure are aided by scientific and cultural innovations from different times and locations: mugshots in eighteenth-century France; mathematical analysis of caste in nineteenth-century British India; innovations by Chinese closed-circuit television companies; and computer vision start-ups conducting bio-security experiments on farm animals.

Building on this social, technical, and historical introduction to FRT, Rita Matulionyte focusses in Chapter 4 on a paramount ethical and legal challenge related to the use of FRT: the lack of transparency around the use and implementation of these technologies by government institutions. By focussing on trade secrets, the chapter examines in which situations these have an ability to inhibit transparency around FRT and whether current limitations to trade secret law, such as a 'public interest' exception, is able to address an emerging conflict between the interests of AI developers who own trade secrets over FRT algorithms and public and experts who demand more transparency around these technologies.

Chapter 5, by Jake Goldenfein, focusses on privacy that has long been central to understanding and addressing the impacts of facial recognition and related technologies. This chapter criticizes the 'representational' understanding of images embedded in current privacy and data protection, which leads to confusion and diversity in the juridical treatment of facial recognition, and the declining coherence of legal concepts. The author suggests that online images are better understood as 'operational' and demonstrates how privacy law's failure to accommodate this theorisation of images leads to confusion and diversity in the juridical treatment of facial recognition and declining coherence of legal concepts.

The book then moves to another core problem of FRT, its potential bias and discrimination. Written by Marcus Smith and Monique Mann, Chapter 6 rejects the implied objectivity of technology and argues that FRT might result in discrimination both owing to data on which it is trained and as a result of a social context in which it is applied. The authors argue that FRT will continue to advance the established power relations in the criminal justice system, unless both data-based and societal-based reasons for inequality and discrimination are remedied.

In Chapter 7, Monika Zalnieriute examines FRT use in public spaces and demonstrates how FRT can interfere with political freedoms of individuals. She argues for a prohibition on the use of FRT in public spaces owing to their disproportionate interference with fundamental rights; especially rights to peaceful protest and freedom of assembly.

Chapter 8, the final chapter in Part I, written by Agne Limante, examines the emerging use of FRT in a war context. It focusses on Russia's invasion of Ukraine, the first major military conflict in which FRT has been used openly. The chapter identifies available information about current FRT use by both Russian and Ukrainian militaries and governments and examines the potential and risks of the use of FRT in a war situation. Together, the chapters in Part I demonstrate that, despite legitimate intentions to achieve security and other public policy goals, governments' use of FRT poses significant ethical and legal risks that require urgent attention.

Part II, 'Facial Recognition Technology across the Globe: Jurisdictional Perspectives', explores how increasing deployment of FRT in public spaces is perceived in different jurisdictions over five regions. It also investigates what regulatory initiatives are in place to address the challenges posed by FRT to fundamental rights and the rule of law, and what approaches could be adopted in the future. Part II consists of eleven chapters and examines FRT use and regulation in Europe (the EU as a separate jurisdiction, United Kingdom, Germany, and Lithuania), North America (United States), South America (Brazil), the Asia-Pacific (China, Australia, and New Zealand), and Africa (Morocco). Its broad geographical reach enables readers to understand how experts around the world – in democratic and authoritarian regimes, in developed and developing jurisdictions – perceive challenges caused by FRTs, and how they judge the actions different governments take to address FRT challenges that have been identified and discussed in Part I.

Part II opens with two chapters analysing legal challenges raised by FRT in the context of EU law. In Chapter 9, Simone Kuhlmann identifies different uses of FRT by governments around Europe, highlights the legal challenges around such uses, and then examines whether and to what extent government use of FRT can be accepted under current EU law. Chapter 10, by Paul de Hert and Georgios Bouchagiar, goes one step further, calling for concrete rules to ban, halt, sanction, or frame specific FRT uses that interfere with fundamental human rights, including the right to privacy and personal data protection. The contribution emphasizes the global reach, risks, and possible global harms of facial recognition technologies, and calls for concrete law-making and uniform enforcement in the field.

The book then moves to specific European jurisdictions, with two chapters focussing on FRT in the UK. Chapter 11, by Nora Ni Loideain, focusses on *Bridges* v. *South Wales Police*, the world's first case examining the legality of a facial recognition system deployed by police, and examines the adequacy of judicial interpretation adopted in the case. In Chapter 12, Giulia Gentile provides an overview of sociological and regulatory attitudes towards FRT in the UK, discusses the *Bridges* saga and its implications, and offers reflections on the future of FRT regulation in the UK.

From the UK we travel to continental Europe. In Chapter 13, Andreas Engel explores the legal framework for the use of FRT in the public sector in Germany, with a particular emphasis on the pertinent German data protection and police laws. The chapter examines German constitutional framework for FRT and whether the current laws in Germany provide a sufficient 'legal basis' that is required for FRT use to avoid the infringement of fundamental rights. The European discussion is concluded with Chapter 14 on FRT regulation in a Central-Eastern European country: Lithuania. Eglė Kavoliūnaitė-Ragauskienė's contribution analyses the lack of specific regulation of FRT use under Lithuanian laws, and draws attention to a minimal public discussion and NGO involvement on this topic. The chapter emphasizes the need for more public awareness around the challenges associated with FRT, which is necessary to push for adequate regulation in the field and its effective implementation.

The next two chapters focus on FRT regulation in selected jurisdictions in North America (United States) and South America (Brazil). In Chapter 15, Mailyn Fidler and Justin (Gus) Hurwitz discuss the current state of laws regulating FRT in the United States. They analyse general laws there, such as those that regulate the use of biometrics, and those that more specifically target FRT, for example, laws that prohibit the use of such technologies by law enforcement and state governments. Particular attention is given to the different regulatory institutions in the United States, including the federal and state governments and federal regulatory agencies, as well as different treatment of governmental and private users of FRT. In Chapter 16, Luca Belli, Walter Britto Gaspar, and Nicolo Zingales provide an overview of the current status of FRT regulation in Brazil, where numerous cities are using FRT in a bid to automatise the public safety, transportation, and border control sectors. It discusses the minimal and incomplete guidance for FRT use found in general frameworks or sectoral legislation in Brazil, and examines whether current rules allowing FRT use for public safety, national defence, state security, investigative activities, and the repression of criminal activities are reasonable and justified.

The last three chapters of the book focus on the Asia-Pacific region and Africa. In Chapter 17, Jyh-An Lee and Peng Zhou overview government use of FRT in China and analyse laws regulating FRT use by private entities. They argue that a recent decision in *Guo Bing v. Hang Zhou Safari Park* that restricts the use of FRT in the private sector does not sufficiently limit surveillance as it does not apply to public authorities. Chapter 18, on FRT in Australia and New Zealand, by Nessa Lynch and Liz Campbell, acknowledges the potentially detrimental and discriminatory impacts that FRT use by the state might have and advance discussion on what principled regulation of FRT might look like. The authors argue that it should be possible to prohibit or regulate unacceptable usage while retaining less hazardous uses of FRT, and propose approaches to how such regulation could be achieved.

Chapter 19, by Sylvia I. Bergh, Isaam Cherat, Francesco Colin, Katharina Natter, and Ben Wagner, examines FRT use and regulation in Africa, with a focus on Morocco. The authors argue that Morocco serves as an example of how technologies such as FRT are becoming key tools of governance in authoritarian contexts.

Based on qualitative fieldwork, including semi-structured interviews, observation, and extensive desk reviews, this chapter focusses on the role played by AI-enhanced technology in urban surveillance and the control of migration between the Moroccan-Spanish borders. The authors highlight the lack of transparency, institutional oversight, and public debate on FRT, and demonstrate how AI-enhanced surveillance is a matter where private interests of economic gain and public interests of national security collide with citizens' human rights.

Overall, this timely and innovative interdisciplinary book encourages a global dialogue on FRT among leading scholars from around the world, with the purpose to inform policy and regulatory debate on these challenging technologies.

CAMBRIDGE

Cambridge University Press & Assessment
978-1-009-32119-8 — The Cambridge Handbook of Facial Recognition in the Modern State
Edited by Rita Matulionyte, Monika Zalnieriute
Excerpt
More Information

PART I

Facial Recognition Technology in Context: Technical and Legal Challenges

CAMBRIDGE

Cambridge University Press & Assessment
978-1-009-32119-8 — The Cambridge Handbook of Facial Recognition in the Modern State
Edited by Rita Matulionyte, Monika Zalnieriute
Excerpt
More Information

1

Facial Recognition Technology

Key Issues and Emerging Concerns

Neil Selwyn, Mark Andrejevic, Chris O'Neill,
Xin Gu, and Gavin Smith

1.1 INTRODUCTION

Facial recognition technology (FRT) is fast becoming a defining technology of our times. The prospect of widespread automated facial recognition is currently provoking a range of polarised responses – from fears over the rise of authoritarian control through to enthusiasm over the individual conveniences that might arise from being instantly recognised by machines. In this sense, FRT is a much talked about, but poorly understood, topic of contemporary social, political, and legal importance. As such, we need to think carefully about exactly what 'facial recognition' is, what facial recognition does, and, most importantly, what we as a society want facial recognition to become.

Before this chapter progresses further into the claims and controversies surrounding FRT, a few basic definitions and distinctions are required. While various forms of technology fall under the broad aegis of 'facial recognition', we are essentially talking about technology that can detect and extract a human face from a digital image and then match this face against a database of pre-identified faces. Beyond this, it is useful to distinguish three distinct forms of facial technologies that are currently being developed and implemented. First, and most widespread to date, are relatively constrained forms of FRT that work to match a human face extracted from a digital image against one pre-identified face. This 'one-to-one' matching will be familiar to the many smartphone users who have opted for the 'Face-ID' feature. The goal of one-to-one matching (sometimes termed 'verification' or 'authentication') is to verify that someone is who they purport to be. A smartphone, for example, is programmed to ascertain if a face in front of the camera belongs to its registered user (or not) and then unlock itself accordingly (or not).

In this manner, one-to-one facial recognition makes no further judgements beyond these repeated one-off acts of attempted identification. Crucially, the software is not capable of identifying who *else* might be attempting to unlock the device. In contrast, a second 'one-to-many' form of FRT is capable of picking a face out of a crowd and matching it to an identity by comparing the captured face to a