

## Book Review

# Mark Andrejevic and Neil Selwyn (2022) *Facial Recognition*. Cambridge: Polity Press

**Pedro Zucchetti Filho**

Australian National University, Australia

**ISBN: 150954732**

Authored by leading experts in facial recognition in Australia, *Facial Recognition* presents a comprehensive account of the diversified facial recognition technology (FRT) applications in multiple scenarios. Andrejevic and Selwyn draw on interesting contemporary examples, such as FRT usage by employers seeking to analyse a job applicant's compatibility, retail stores aiming to detect clients' satisfaction and preferences, and law enforcement and intelligence agencies.

The book is neatly structured, consisting of a preface, the main body (comprising seven chapters) and an epilogue. The authors helpfully address FRT's main characteristics in the first two chapters, in addition to clarifying its historical development and delineating its essential concepts.<sup>1</sup> The third chapter focuses on analysing FRT's global application.<sup>2</sup> The fourth, fifth and sixth chapters scrutinise the pros and cons of the technology, seeking to understand its potential benefits and harms.<sup>3</sup> The last chapter critically evaluates FRT from an individual and societal point of view.<sup>4</sup> Finally, in the epilogue, the writers share their perspectives concerning possible future FRT deployment and implementation paths.<sup>5</sup> Considering the diversity of FRT problems extensively tackled in the book and the richness of the analysis, I have decided to narrow my focus in this book review to parts of the analysis that appealed to my interest as a legal scholar working on the deployment of FRT in Brazil.

In the introduction, Andrejevic and Selwyn emphasise two of the most significant implications of FRT deployment that are repeatedly addressed throughout the book: the prospect of an omnipresent surveillance state and the establishment of a new stage in our comprehension of privacy. The authors perceive that FRT establishes a decisive shift in monitoring capability caused by the promise of ubiquitous and remote identification.<sup>6</sup> They demonstrate what society can expect from the pervasive deployment of this cutting-edge tool, indicating that, eventually, people will need to choose between the maintenance of their privacy and anonymity in public spaces and the promises of FRT, namely an increase in efficiency, convenience, security and control.

In the same section of the book, the authors analyse the historical development of FRT, specifically, the computational techniques for developing facial matching.<sup>7</sup> The most relevant people in this regard were the United States (US) researcher

<sup>1</sup> Andrejevic, *Facial Recognition*, 1–55.

<sup>2</sup> Andrejevic, *Facial Recognition*, 56–77.

<sup>3</sup> Andrejevic, *Facial Recognition*, 78–158.

<sup>4</sup> Andrejevic, *Facial Recognition*, 159–180.

<sup>5</sup> Andrejevic, *Facial Recognition*, 181.

<sup>6</sup> This dystopian scenario made Nora Khan designate FRT as the 'machine eye', in which images of people are uninterruptedly surveilled, labelled, sorted, and analysed by computerised technology (Andrejevic, *Facial Recognition*, 21).

<sup>7</sup> Andrejevic, *Facial Recognition*, 1–25.



Except where otherwise noted, content in this journal is licensed under a [Creative Commons Attribution 4.0 International Licence](https://creativecommons.org/licenses/by/4.0/). As an open access journal, articles are free to use with proper attribution. ISSN: 2652-4074 (Online)

Woodrow ('Woody') Wilson Bledsoe and his collaborators Helen Chan Wolf and Charles Bisson, who spent significant time in the 1960s working 'under the guise of the Panoramic Research company based in Palo Alto'.<sup>8</sup> As explained by the authors, the scientific approach during the 1960s and 1970s focused on establishing the primary capabilities of FRT. These priorities only changed between the 1990s and 2010s, at which point the attention mostly turned to exploring commercial opportunities. Moreover, the scholars demonstrate that during this time, FRT's large-scale application started to affect our private lives and social interactions in an unprecedented way.<sup>9</sup>

While the book's introduction explains FRT's technical and commercial evolution, Chapter 2, 'Facial Recognition: Underpinning Concepts and Concerns', analyses its distinct capabilities or functionalities.<sup>10</sup> The authors detail three different capabilities of FRT.

The first, the *verification task*, addresses the question of whether someone is who they say they are. It is also called a one-to-one (1:1) matching because the image of the person claiming to be who they are is compared to one located in a document.<sup>11</sup> Authentication is the aim. The second, the *identification task*, is a much more intricate process. In contrast with authentication, this is a one-to-many or one-to-all (1:n) matching process. In practical terms, the matched image is usually found in previous photographs located in large databases, such as national ID cards. Finally, the third capability is *facial analysis*. This involves inference; that is, it seeks to distil the unique characteristics of a person as well as what emotions they might be feeling.<sup>12</sup> According to Andrejevic and Selwyn, when the *verification task* fails (when FRT misidentifies someone), it has the potential to bring considerable negative consequences to people, such as denial of access to health assistance and sources of credit. A similar risk is evident when the *identification task* is at play. However, in this case, the consequences can be even more severe because this functionality is commonly deployed by intelligence and law enforcement agencies to identify suspected criminals.<sup>13</sup>

Andrejevic and Selwyn strongly criticise the idea of technological neutrality throughout Chapter 2. According to them, the increased adoption and (mis)use of FRT by law enforcement agencies during the last decade proves how inaccurate and untrue it is to affirm that these technologies are merely neutral tools.<sup>14</sup> The chapter also briefly explores biased outcomes—highlighting the propensity of FRT systems to misrecognise people of colour and other demographics—and the unlikelihood of these being eliminated. Specifically, the authors demonstrate that FRT is a device conceived and developed by human actors. Therefore, subjectivity is the norm and objectivity the exception. From the authors' perspective, the idea of creating a neutral and objective FRT system is a fantasy because FRT developers cannot entirely surmount their biases and prejudices, which are intentionally or unintentionally installed in the machine. This is why establishing robust legal mechanisms and safeguards is so essential. Chapter 3, 'Mapping the Facial Recognition Landscape', explains how different commercial entities<sup>15</sup> and government institutions<sup>16</sup> are central to any critical discussion of the recent rise of FRT and its future development. Additionally, this chapter

<sup>8</sup> Andrejevic, *Facial Recognition*, 6. In the end, Panoramic Research had a more pragmatic approach, developing FRT's capability for various military intelligence and law enforcement applications. Bledsoe's work concerning FRT was ground-breaking, and the book gives a detailed account of his accomplishments.

<sup>9</sup> The expansion of its use, caused by a shift in the surveillance landscape concerning risk detection and management, came especially after the 9/11 attacks in the US, which announced a new meaning of threat assessment. It was the official start of the war on terror, which heralded various new threats. Given this context, it is worthwhile to note that the authors problematise FRT deployment in various situations and explain why society must carefully consider adopting FRT. In other words, they demonstrate how surveillance technologies are dangerous to human rights and civil liberties (e.g., freedom of movement, freedom of association and assembly, and right to equality and non-discrimination), especially because FRT systems are fallible, intrusive, and prone to cause function creep (Andrejevic, *Facial Recognition*, 97–103).

<sup>10</sup> Andrejevic, *Facial Recognition*, 26–55. The authors approach this subject once more in pages 144–149, examining these functions through a new lens and aiming to explain how large-scale FRT deployment will inevitably lead to the stratification of the physical spaces and the strengthening of social inequalities.

<sup>11</sup> Andrejevic, *Facial Recognition*, 28.

<sup>12</sup> The literature broadly explores facial analysis features, which profusely indicates how the inferences made are often invalid—in some cases, even operationalising outdated theories of phrenology and physiognomy. This third functionality, as well as its serious consequences, is strongly criticised by the authors (Andrejevic, *Facial Recognition*, 133).

<sup>13</sup> Davis, *Facial Recognition Technology*, 12.

<sup>14</sup> As pointed out by the authors, human subjectivity and its prejudices play an essential role in the outcome of an algorithmic model. This means the developers' worldviews will be reflected in the development of FRT models. The harms and mistaken outcomes will continue appearing because these tools are deployed in a biased society. In other words, biased results happen precisely because we live in a biased context imbued with "uneven social relations" (Andrejevic, *Facial Recognition*, 135).

<sup>15</sup> These entities mainly encompass the GAFAM corporations (Google, Apple, Facebook, Amazon, and Microsoft).

<sup>16</sup> One of the government institutions mentioned is the US National Institute of Standards and Technology (NIST), which is responsible for supervising the ramifications of software development and emerging technologies and which has played an important role in overseeing the

addresses the issue of government involvement in facial recognition, emphasising that FRT development was accelerated by US government funding and support from specific agencies.<sup>17</sup> Therefore, this chapter scrutinises the role of corporations and government agencies in advancing improvements in FRT. The chapter also briefly discusses the topic of oversight and regulation. Many jurisdictions are considering various legislative interventions. The authors provide some insights on the European Union's General Data Protection Regulation (GDPR) and some other legislative proposals currently being considered globally, such as calls for a ban or a moratorium on the use of FRT.<sup>18</sup>

In Chapter 4, 'Pro-social Applications', the authors seek to answer whether FRT has a 'good' application. They raise the question of whether a massive installation of these devices is possible without simultaneously seriously jeopardising civil rights and causing large-scale discrimination. Thus, the authors assess whether society can feasibly attain a proper balance.<sup>19</sup> Throughout the remaining part of Chapter 4, the authors address FRT deployment in a wide variety of scenarios, such as in casinos, retail stores,<sup>20</sup> schools, workplaces and hospitals. In addition to explaining FRT's diversified applications, they also address three significant characteristics that society should consider before deciding to adopt FRT on a large scale.

The first characteristic, and unlike what is espoused by common sense, is that FRT is fallible. Although the statistical number of false positives and negatives remains low, a significant number of people continue to be erroneously identified by these systems despite the advances in technological development. The second characteristic of FRT relates to 'function creep', meaning its application to purposes distinct from the original applications<sup>21</sup>. FRT enables constant monitoring, recording and tracking, and these functions can strengthen authoritarian regimes. Following this line of reasoning, authoritarianism could (and can) occur even in democratic countries. The topic relates to 'purpose limitation', one of the core principles of data protection laws. The third intrinsic characteristic is FRT's intrusiveness. What might appear to occur exclusively in the realms of science fiction decades ago is now something that has become a reality: reconstructing the timeline of any person. Unlike CCTV cameras, FRT enables more granular surveillance and, consequently, makes it possible to collect information concerning a person's participation in specific events.

Chapters 5 and 6 offer strong arguments justifying why it is not feasible to want to 'fix' FRT, nor to make it 'fairer'. In doing so, the authors explore one of the main problems associated with FRT's biased outcomes: how databases are created. The authors clarify how the challenges faced by computer scientists are not only technical but also social, which makes algorithmic bias even harder to eliminate. More specifically, Chapter 5, 'Problematic Applications: Facial Recognition as an Inherent Harm?', addresses issues such as how biometric information has been used in criminal investigations for decades. Here, we can consider examples like the use of fingerprint and DNA analysis.<sup>22</sup> Moreover, in this chapter, Andrejevic and Selwyn succinctly clarify why FRT has become so attractive to law enforcement agencies. Chapter 6, 'Facial Features: Emerging Promises and Possible Perils', addresses the concerns related to the fact that our faces are becoming metadata. The reformulation of human interactions would be an inescapable consequence in a society where our faces would be considered the 'prime sources of personal information'.<sup>23</sup> The authors speculate about these effects and their repercussions, which helps shed light on the dangers of this technological tool.

In the final chapter, 'Making Critical Sense of FRT and Society', Andrejevic and Selwyn point out the necessity of a holistic approach to guarantee a safer development and deployment of FRT systems. According to the authors, this would require 'ongoing conversations'<sup>24</sup> involving computer scientists, policymakers and civil society organisations. The authors consider that such conversations would offer a significant step towards a more substantial understanding of FRT's complex issues. Andrejevic and Selwyn finish the book by sharing three possible scenarios: the path of least resistance, complete prohibition,

---

unfolding of digital innovation since the 1980s. NIST's primary function is to evaluate the most recent FRT systems to verify their accuracy and reliability. Considering it has a relevant role as an institution responsible for evaluating FRT systems, it also performs the role of establishing standardised practices worldwide as an official guarantee of the efficiency and effectiveness of the latest systems.

<sup>17</sup> Andrejevic, *Facial Recognition*, 60.

<sup>18</sup> Andrejevic, *Facial Recognition*, 73.

<sup>19</sup> Andrejevic, *Facial Recognition*, 79.

<sup>20</sup> FRT is used to augment these monitoring and surveillance systems in this context and aims to help identify shoplifters. One example of how FRT can enhance CCTV capabilities is the United Kingdom's Facewatch system, through which the device sends a signal or alert to the shopkeeper when somebody entering the store is rated a subject of interest based on information collected from Facewatch's national database (Andrejevic, *Facial Recognition*, 87).

<sup>21</sup> The phenomenon is deeply analysed by Bert-Jaap Koops in a paper addressing specifically the clarification of the concept "The Concept of Function Creep."

<sup>22</sup> Andrejevic, *Facial Recognition*, 111.

<sup>23</sup> Andrejevic, *Facial Recognition*, 142.

<sup>24</sup> Andrejevic, *Facial Recognition*, 160.

and robust and open scrutiny.<sup>25</sup> Each of them will bring varied consequences. Regardless of the chosen path, it is crucial to remember that FRT is a device with profound implications for democracy, privacy, autonomy and its corollaries, such as free speech and freedom of assembly. The authors suggest some ‘remedies’ to mitigate these issues, such as regular testing for bias and accuracy by independent regulatory authorities.

FRT must be used only in transparent and accountable ways, and its use must comply with data protection and privacy legislation. Numerous legislative frameworks on privacy and data protection already exist, but the authors argue that they need to be more effective in practice. Lack of public awareness and political will can be considered two of the causes for the failure to address some of the concerns raised by FRT. However, it should be acknowledged that privacy and data protection legislation can only go so far. Frameworks such as the European Union’s GDPR have specific carve-outs for areas like national security. It is relevant to note that the authors’ thorough analysis of the consequences of a large-scale FRT deployment, such as the creation of a mass surveillance state in which liberty and autonomy are threatened, may, therefore, require an alternative legal solution. Such examples raise clear concerns for human rights—for example, the right of assembly and association and freedom of speech and movement—due to their capacity to significantly constrain behaviour due to the chilling effects of surveillance. In this respect, the book offers examples of countries that adopted FRT to covertly track protests inside their territories, such as the surveillance of ethnic minorities in China.<sup>26</sup>

Leaving these specific issues to one side, the authors also suggest that more than just robust legislation is needed. Oversight bodies and civil society organisations must have access to information concerning FRT’s deployment data, enabling them and other actors to target bad-faith FRT deployments. Finally, as demonstrated by the authors, the commercialisation of FRT has increased significantly in the last decade, and it would be advisable that society does not allow democracy and human rights to be surpassed by an appetite for profit. Above all, it is indispensable that FRT’s developers and designers are appropriately informed about the social issues raised by this technology so they can develop a solid commitment to maintaining democratic values.

This book makes an important contribution to the FRT literature. The rich analysis offered will be highly relevant to those interested in broadening their understanding of FRT. Although it is a technical book, it should be considered valuable to anyone seeking to understand FRT holistically and its numerous implications for us all. For legal scholars, the book offers many opportunities as a foundation to consider the multitude of public and private, international and national law issues posed by the development and deployment of FRT.

## Bibliography

- Andrejevic, Mark and Selwyn, Neil. *Facial Recognition*. Cambridge: Polity Press, 2022.
- Davis, Nicholas, Lauren Perry and Edward Santow. *Facial Recognition Technology: Towards a Model Law* (Human Technology Institute, 2022). <https://www.uts.edu.au/human-technology-institute/projects/facial-recognition-technology-towards-model-law>.
- Koops, Bert-Jaap, “The Concept of Function Creep.” *Law, Innovation and Technology* 13, no 1 (2021): 29-56. <https://doi.org/10.1080/17579961.2021.1898299>.

---

<sup>25</sup> Andrejevic, *Facial Recognition*, 182.

<sup>26</sup> Andrejevic, *Facial Recognition*, 16.