Part of this book was written at the State Library of Victoria in Melbourne and a small amount was written at the British Library in London. Designed by architect Joseph Reed (who also designed the UNESCO World Heritage Royal Exhibition Building in Melbourne), the Victorian library opened in 1856. The La Trobe Reading Room, or ‘Dome Room’, however, where the majority of my time was spent, opened in 1913. At the time it was the largest concrete dome in the world and an advanced piece of technology. The space is striking, not only for its scale and ambiance, but also for the arrangement of desks stretching outwards in rows from a central plinth towards the room’s periphery. The configuration exposes each scholar to an (often absent) invigilator, capable of monitoring the entire area. Although several important features of Jeremy Bentham’s panopticon are absent from this layout, there remains a gentle social pressure ensuring that nobody is talking or writing in the library books. In London, the British Library on Euston Road opened more recently, in 1998. Its reading rooms bear little resemblance to the historic style of the State Library in Victoria. There are no observation posts for staff nor are rooms arranged to ensure the visibility of readers to a central observer. Rather, each room is saturated with a grid of closed-circuit video cameras. Each row of desks is exposed to at least one camera mounted in the bulkhead, monitoring the length of the row, with more cameras on orthogonal walls. Under the electronic eyes of the British Library the feeling is that you are the one being read.

In contemporary life, individuals are exposed to reading – analysis and interpretation by an external agent – in multiple contexts, be it through ordinary human interaction or remotely via technological mediation. Pattern recognition and prediction are intuitive human decision-making processes, and individuals engage these cognitive exercises throughout their interaction with the world. But as our social environments are increasingly mediated by digital technologies, the character of the decision-making that reads and interprets us changes. One significant change is the degree to which those decisions and interpretations are performed by automated agents. Another change is the degree to which knowledge generated by autonomous agents is becoming a central way of understanding.
The integration of computation into everyday life has produced striking social transformations. We now inhabit new infrastructures of ‘planetary scale computation’ that involve massively complex systems of data collection, retention, and processing, and generate immense quantities of knowledge about the world and the people within it. As Mark Andrejevic, Alison Hearn, and Helen Kennedy argue, ‘it is now axiomatic to claim that we are in the “age of big data” and are witnessing a quantitative (and perhaps qualitative) “revolution” in human knowledge, driven by accompanying forms of data mining and analytics’. As many contemporary scholars have shown, this type of knowledge-generating data analysis is visible in credit, and insurance scoring, healthcare, the provision of public services, behavioural advertising, law enforcement and policing, intelligence and security practices, criminal justice decisions like bail, sentencing and parole, employment and human resources practices, and many other areas. Along with whatever benefits these tools might bring to scientific research, the application of methods from the physical sciences to human behavioural analysis means this computational society is also becoming one of social scoring, risk assessment, and predictive policing.

We are also entering a new phase in the nature and scale of data collection and analysis. For decades, the primary stuff of big data, at least for scholars of digital surveillance and privacy, has been the ‘transactional’ data typically created by interacting with online environments. However, this data is increasingly supplemented with data captured directly from the ‘real world’ with sensors, and transformed into understanding through the unique statistical and pattern matching capacities of machine learning and neural networks. These technologies and practices translate the physical world into the symbolic register of computation, while simultaneously producing decisions and classifications that are expressed in the physical world and its objects. Automated agents now look, listen, measure, and act in ways that hybridise informational and physical environments into cyber-physical systems. When those systems include people and their behaviour, that hybridisation requires an understanding of individuals as compatible and co-extensive with the symbolic processing logics of computation and statistical knowledge systems. As the world is translated into computational registers, labelled, classed, categorised, and classified, we thus encounter new epistemologies premised on extremely granular measurement and extremely powerful computation. As the tools develop further,

---

rather than approximating people through reduction and heuristics, data science appears to be embracing a narrative of ‘revelation’ – of expressing the truth about its subjects. This logic of revelation, the idea that humans are best understood through the behavioural and informational patterns they generate, and that those behavioural patterns can be put to work or optimised towards certain goals, are becoming the defining characteristics of contemporary surveillance culture.

**PROFILING**

The primary data inputs for the automated analysis of people are biological and behavioural data. The creation and processing of those datasets, and the law’s response, is the primary material of this book. But the information storage and processing that, it is argued here, began with photography, crude biometrics, and intelligence dossiers, are entering a new phase through the technologies, techniques, and philosophies of data science. The legal language for this type of decision-making, classification, and knowledge generation about people is ‘profiling’. It is non-controversial that profiling as a form of knowledge production is an inherent and necessary element of ordinary decision-making. Reductionist thought processes enable quick, functional choices. The term profiling is etymologically connected to the artistic reproduction of a ‘half face’ (as opposed to a ‘full face’), as well as the more textual notion of summarising a person in writing – both suggesting reductive representations used to capture identity or character. At a broad social level, these decision-making processes include ‘an ongoing distribution and cataloguing of information about the desires, habits, and location of individuals and groups’. Within law enforcement specifically, that manifests as ‘a process whereby behaviours and/or actions exhibited in crime are assessed and interpreted to form predictions concerning the characteristics of the probable perpetrator(s) of the crime’. In certain administrative contexts, these profiling decisions constitute instances of states deploying technologies to count, tabulate, and classify (and thereby define) their subjects, what Ian Hacking calls the idea of making up people. What profiling means in the context of contemporary computational environments is the subject of this book. It is argued that new profiling exercises, while building on the logics, politics, rationales, epistemologies, and techniques of older surveillance systems, also involve new knowledge paradigms and new consequences such as behavioural optimisation and other forms of manipulation. Beyond the epistemic features of ‘big data’ that have elsewhere been summarised as ‘heterogeneous, unstructured, trans-semiotic,

---

decontextualized, [and] agnostic’,10 the way these technologies are put to work, as particularly visible in the application of neural networks to image classification for instance, represents a new type of ‘computational empiricism’, buoyed by new relationships between states and private industry that produces computational products, services, and infrastructures. Profiling in the form of behaviour and personality computation is no longer about categorisation into consumer groups or the creation of credit risk scores, it is about building models of individuals that can direct behaviour towards any end.11 It is about knowing people better than they can know themselves.

On one hand, some scholars reject any inherent problematisation of profiling as a decision-making practice, even in areas where they have been historically controversial like law enforcement.12 For example, Frederick Schauer believes that profiling based on ‘actuarial’ processes (as opposed to ‘clinical’ methods which rely on subjective expert opinion) of ‘attributing to the entire category certain characteristics … that are probabilistically indicated by membership in the category, but that still may not be possessed by a particular member of the category’13 are acceptable following an appropriate cost/benefit analysis. He believes only generalisations without sound statistical basis should be avoided, and accordingly argues that issues of ‘racial profiling’ by police, for instance, are actually problems of racism not of profiling.14 On the other hand, scholars like Bernard Harcourt argue that reliance on statistics in profiling actually produces ‘hidden distortions with significant costs for society’.15 Others have also argued that purely numerical approaches may be ‘iniquitously ideological’ in their promotion of a particular worldview.16 The position taken in this book is that there are consequences to embracing purely numerical and statistical approaches to understanding and assessing people, whether or not those assessments are true or statistically valid. Indeed, the nature of knowledge and decision-making has changed. Traditional opinion and subjective clinical decisions17 are increasingly marginalised in favour

14 Ibid, see, e.g., ch 7 ‘The Usual Suspects’.
15 Bernard Harcourt, Against Prediction: Profiling, Policing and Punishing in an Actuarial Age (University of Chicago Press, 2006) 106. Harcourt argues, for example, that there is an overlooked social cost to profiling which includes the costs of additional incapacitation and incarceration, and that profiling problematically shapes conceptions of justice on the basis of a specific theory of punishment.
17 See, e.g., Barbara Underwood, ‘Law and the Crystal Ball: Predicting Behavior with Statistical Inference and Individualized Judgment’ (1979) 88 Yale Law Journal 1408 where she defines ‘clinical’ approaches at 1432: ‘One way to describe the difference between clinical and statistical methods is to
of ‘machinic objectivity’, and ‘judgement’ is replaced by computation. The belief that purely computational mechanisms offer the most desirable pathways to knowledge also reflects an ideological and political commitment likely to favour entities with the largest computers. An all-out rejection of the actuarial or statistical paradigm, however, seems less and less realistic, indicating the need to conceptualise new mechanisms within this model of governing that show a capacity to reduce its problematic effects.

The legitimacy of a profiling exercise is the domain of law. Legal regimes form part of the environment in which the merit of particular ways of knowing are evaluated. Legal regimes facilitate or constrain technologies, practices, and ideas. This book accordingly examines contemporary profiling techniques, and their antecedents, as figures in the law and legal thinking, as well as the legal formulations that have emerged as a result. The legal fields in which these responses are most visible include the information law domains of ‘privacy’ and ‘data protection’, as well as the emerging paradigm of ‘algorithmic accountability’. As the technologies, techniques, and narratives behind profiling change, we similarly see shifts in the legal doctrines addressing these systems. Legal limitations on surveillance and profiling have historically sought to reduce exposure to observation, increase transparency in data collection, retention, and profiling, and now, insist on fairness and interpretability in human computation. In other words, law has addressed profiling as a way of knowing by preventing access to individuals (or storage of information that might lead to certain decisions); by affording surveillance subjects the right to participate in the generation of knowledge about them; by ensuring that technical systems encode the world and the people within it according to certain statistical definitions of fairness; and potentially insisting on explanation of how automated profiling and decision-making systems achieve their outputs. Further, as the substance of legal protection has changed, we also see the actual formats and technologies of law evolve. For instance, whereas traditional privacy actions are connected to constitutionally protected individual rights, data protection also embraces diffuse bureaucratic compliance tools. The emerging fields of fairness and accountability change the nature of legal enforcement again, by embracing infrastructural and technological implementations that challenge traditional understandings of what constitutes law, legality, and legal subjectivity.

This book tries to account for, and contextualise, the emergence of these legal responses to profiling by understanding the technological narratives to which they are oriented. In doing so, the book also demonstrates how and why say that clinical methods pay more attention to individual applicants, and statistical methods pay more attention to the rules for selecting them.'

18. Hacking, above n 8, 3. The full quotation reads: ‘Probability cannot dictate values, but it now lies at the basis of all reasonable choice made by officials. No public decision, no risk analysis, no environmental impact, no military strategy can be conducted without decision theory couched in terms of probabilities. By covering opinion with a veneer of objectivity, we replace judgment by computation.’
contemporary profiling practices transcend the legal tools we presently have to limit their effect. That transcendence, it is argued, is a product of the way contemporary profiling and data science practices construct and enact certain narratives of the self and identity. Those narratives, while increasingly accepted in the politics and practices of governing, are what the dominant legal paradigms reject, but with less and less success. How to re-think the shape and utility of legal notions of identity within a changing technological context is thus a critical question animating this book.

INFORMATION LAW AND IDENTITY

One influential understanding of privacy, data protection, and even algorithmic accountability, in their application to profiling, is that these legal systems protect individuals by protecting ‘identity’. That is, law operates to prevent an entity from improperly constructing a subject identity and making it the basis for further decision-making. For example, privacy law, at least in European privacy jurisprudence, has played a role in imposing limitations on what state entities can retain in administrative and law enforcement filing systems in order to prevent stigmatisation. This is a different deployment of privacy law than preventing the unauthorised disclosure of private information, intrusion on seclusion, or even protections of reputation. The protection of identity is not necessarily concerned with the dissemination of private information or the production of a problematic public image. Rather, these legal regimes operate to limit certain interpretive exercises by restricting what information can be used to make decisions. Data protection similarly protects identity by affording a degree of transparency over retained information. Data protection, or ‘information privacy’ regimes typically provide ‘data subject rights’ for eliminating inaccuracy or irrelevance in data holdings. Those rights enable individuals to impose their own self-image into data-processing environments by ensuring retained data somehow corresponds to the data subject’s understanding of themself.

That in certain technological contexts, privacy might be best understood as a ‘freedom from unreasonable constraints on the construction of one’s own identity’ has therefore been a theme in the information law scholarship since at least the 1990s. For instance, Robert Post saw privacy’s protection of ‘autonomy’ in ‘the ability of persons to create their own identity and in this way to define

Benjamin Goold argued that privacy ‘is not simply about the keeping of secrets or the restriction of access to information. Rather, it is also about maintaining a degree of control over one’s identity’. And Mireille Hildebrandt has claimed that in the era of profiling, privacy’s connection to identity ‘seems a more apt way to define privacy than definitions that focus on the sharing of personal data or on adherence to the purpose specification and the purpose limitations principles’. However, ‘identity’ is also an exceedingly difficult concept to define, let alone operationalise in law. Indeed, it is argued here that the mismatch between notions of identity that animate existing legal protections and how contemporary data science conceptualises identity are causing what feels like a further loss of legal control over technological practices.

Ideas of identity deployed in the legal analyses are typically derived from certain philosophical models of identity, particularly ‘narrative’ theories. Scholars interrogating the relationship between information law and identity often invoke the work of Paul Ricoeur, and his notions of ipse and idem identity to provide an account of the multifaceted dimensions of identity construction. This division between ‘self’ and ‘sameness’ identity, elsewhere contextualised as ‘narrative’ and ‘categorical’ identity, and even ‘internal’ and ‘external’ identity, structures the legal ideas that address when ‘these two conceptions of identity come into competition’, or ‘when the categorical overlaps, contradicts and supplants the narrative’. Goold, for instance, describes how certain surveillance practices generate a threat to identity that may be actionable in law, when ‘an increasingly sophisticated array of surveillance and data processing techniques, which enable information to be acquired and shared at almost zero-cost . . . threaten to establish the “categorical identity” as the primary means by which we are known – to the state and, more disturbingly, to each other.’

The correspondence between internal and external life and appearance, the duality of identity, and its relationship to law and images, also has roots in psychoanalytic arguments by authors like French jurist Pierre Legendre. In retelling the story of Narcissus in his Introduction to the Theory of the Image, Legendre describes how the body is only presented for perception by others through means of an image. He argues that through the body’s translation into representation, it loses its status as a biological object and becomes something fictional or constructed, and

---

26 In particular, Paul Ricoeur, Oneself as Another (University of Chicago Press, 1992).
27 Goold, above n 24, 63.
28 Ibid 68.
that the self-produced subject only emerges through being a target of seeing – that is, an object seen by someone else. Roland Barthes famously explored similar effects instituted by the camera in *Camera Lucida*, describing the photograph as the advent of the self as other – ‘a cunning dissociation of consciousness from identity’\(^{30}\) – and the experience of being photographed as a transformation from subject into object, whereby ‘others – the Other – do not dispossess me of myself, [rather] they turn me ferociously, into an object, they put me at their mercy, at their disposal, classified in a file, ready for the subtlest deceptions’.\(^{31}\) The reification and loss of control over those sites of outward appearance, and the transformation of an individual into an object and its classification in a file, thus threaten identity by being inimical to the way that subjects produce themselves – as argued by Cornelia Vismann, ‘by administering themselves – by establishing a feedback with their own actions’.\(^{32}\) Finding ways to give authority to that internal subjectivity has so far been the primary legal goal in this context.

For our purposes, there is also something significant in the relationship between images and data, especially images in the form of numerical data (i.e. as measurements). For instance, Giorgio Agamben identifies a turning point in the social and technological understanding of identity when individuals and their images were subjected to anthropometrics and biometrics.\(^{33}\) The invention of photography and biometrics is where Agamben locates the end of external identity as a product of how we are recognised socially, and the beginning of a new institutional construction of identity informed by surveillance images and measurements. With the biometrics of Alphonse Bertillon (described in Chapter 2), Agamben argues ‘for the first time in the history of humanity, identity was no longer a function of the social “persona” and its recognition by others, but rather a function of biological data, which could bear no relation to it’.\(^{34}\)

For Agamben, biometrics represent a critical turning point in identity construction, especially in their function of making identity registers and archives searchable, and their being put in service of building institutional mechanisms for knowing people. That institutional capture of outward identity also commenced the elimination of space for an ‘ethical’ relationship to the image, a space for interpretation between the internal narrative of the individual and their outward appearance. It thus generated, in Agamben’s words, ‘naked life, a purely biological datum’, or ‘identity without the person’. This process of eliminating the interpretive space between individual and image that began with photography and anthropometrics has only amplified with the biometric and behavioural data analyses performed by

---


\(^{31}\) Ibid 14.


\(^{34}\) Ibid 50.
Building the World State

machine learning, in the service of commercial, political, and law enforcement endeavours. Antoinette Rouvroy describes the result of this ‘crisis of representation’ in our contemporary political and economic paradigm, noting:

There is no longer any subject in fact. It is not only that there is no longer any subjectivity, but it is that the very notion of subject is itself being completely eliminated thanks to this collection of infra-individual data; these are recomposed at a supra-individual level under the form of profile. You no longer ever appear.35

In many ways, the capture of biometric (as well as behavioural) data was the beginning of the end of identity defined by representation – that is, as defined by a separation between the thing and its appearance. That separation has only further disappeared in institutional identity’s encounter with computation.

Since the Second World War, the discipline of cybernetics, in its various expressions and iterations, has generated new understandings of identity and self, technologically oriented more around computation than images. This intellectual tradition, informed by inter-disciplinary collaboration between communications, mathematics, biology, and engineering, as well as neuro, behavioural, and cognitive sciences, conceptualised the human mind as a symbolic information-processing machine, that could be modelled in purely informational and computational terms, and extended into information-processing networks.36 As we will see, narratives of total human computability and control, but also new models of human autonomy, emerge from the shadow of cybernetic thinking. Central to these ideas however, in both their troubling and more emancipatory expressions, is a rejection of the person behind the mask as an unknowable and mysterious kernel of inward ‘self’ identity, and an embrace of identity as a systemic concept defined by dynamics of information flow.

BUILDING THE WORLD STATE

The ‘world state’ is a metaphor. It is not intended to denote the existence of a global single state or ‘new world order’. That said, it does reference the changing nature of state-hood, the fact that geographic designations of jurisdiction and sovereignty have become increasingly strange, and that what we once associated with the state can now be described as a register of governance enacted by both traditional institutions as well as technology platforms. To that end, authors continue to explore how the ascendance of ‘platform sovereignties’, and the reality of infrastructures adopting sovereign registers of their own, means dealing with the challenges that planetary-


scale computation poses to law’s geographic and jurisdictional legacies. However, the primary use of the ‘world state’ metaphor here is to describe a process and condition by which the physical world, the objects and people within it, and their internal capacities and propensities, are translated into, and represented within, the symbolic register of computation. The phrase is taken from a computer vision textbook describing the outcome of an automated classification process. The world (x) is measured and analysed, and a ‘world state’ (w) is produced. This metaphor also builds on long-standing thinking in media studies about how technologies and images that were intended to provide insight about the world ultimately end up blinding us. The ‘world state’ is what happens when the proliferation of technical images turns the world into an image, a collection of what Vilém Flusser calls ‘states of things’, or where images become the only path to ‘the real’. This classic critique of technology insists that technological mediation inhibits access to ‘the real’ or ‘the event’. In the case of photography, for instance, we are reminded that the images we create, while intended to be windows or maps for understanding the world around us, actually operate more like screens. Rather than expose the truth of the world, our images saturate the world, producing a veneer under which ‘the real’ slowly decays. A form of this critique is often levelled at profiling, wherein data produced through interactions with information environments are used as proxies for defining particular characteristics about us. Critiques of this ‘scored society’ describe how scores inadequately capture or represent us as individuals, and that proxies result in reduction, distortion, and error. This intervention frames the harm to persons from profiling in terms of loss or reduction through representation.

In the computational society of the ‘world state’ – mapped by innumerable sensors that capture vision, sound, motion, and interactions with information systems – technology becomes more than a just system of representation. The ‘world state’ is not simply an informational layer that exists on top of, or adjacent to, the physical or ‘real world’ – it is enactive, it works, it governs, it decides. The result is a composite of physical and informational places, persons, and rules into networks of cyber-physical systems. The ‘world state’ is thus the dynamic and recursive cyber-physical reality that we increasingly inhabit and navigate. It is the contemporary iteration of

37 Bratton, above n 1.