1 Introduction

Let's start our journey with a question – a simple one: what have you done today? Take a second to think about it before you read on.

You have probably got out of bed as a starter. How did you sleep? You have probably already prepared for your day. Maybe you are the early-starter type, so you are straight into the shower, dressed and off to the kitchen to make breakfast. What did you have for breakfast? Perhaps something that involved fishing in a fridge or using a kitchen device such as a kettle, a coffee machine or a toaster. You may have younger mouths to feed also, nappies to change or school lunch boxes to prepare – all before you head off to work, wherever and in whatever form that may take. And as you progress during your day, you have the bings and beeps of your smartphone as you negotiate your life and try to understand the world around you. Maybe you need to order a taxi or an Uber. Maybe you need to shop or withdraw cash. Maybe you need to make a call or send a text, attend a meeting or pick up the kids – or the many other things that now pack our expected lives.

Now let me ask you this: what did you do this day last week? Possibly similar activities but maybe something different. What about this date last month or even last year? It gets harder to distinguish one day from the next, unless something of note has occurred.

But what if we lived in a world where data about everything was collected? What if all devices, all buildings and all infrastructures were sensorised?

It could be a smarter world. We would know more about our own patterns and foibles, as we could easily compile a historical record of all our activities. We would no longer struggle to work out what we did today, last week, last month or anytime previously. It would all be recorded: the times we boil the kettle for our morning cup of tea, how we travel to work and when we travel – maybe even the days we feel sad, indicated by the movies we watch or music we listen to.

Smarter still, these types of sensor data can also be used collectively and not just individually. So, your repetitive kettle use, at the same time

each morning, can be fed into electricity usage across the broader population's grid. We can work out travel patterns of communities or populations by tracking individual smartphones to better allocate resources. We can even consider the mental health of individuals in seemingly massive populations by monitoring social media and activities in other public fora.

'Smartness' in the smart world thus connotes prediction and prescription: prediction, in that we can better assess how individuals, communities and populations will act, behave and possibly even feel; prescription, in that we can target outcomes to better meet predicted futures.

The smart world obliquely consists of pervasive collections of data from a vast range of sensorised devices, infrastructures and environments. It puts us on a path where data about everything could be collected for smartness to function and flourish. The success of the smart world is consequently dependent upon vast scales of data collection, particularly from sensorised devices. The smart world is therefore the 'collected' world. But what does it mean for us to live in a collected world? How do we make sense of it?

1.1 The Book's Thesis

A common frame for addressing these questions is information privacy or data protection law because it directly governs our relationship with the many data collectors of the smart and collected worlds. Different concepts of information privacy exist, but its traditional and dominant form regards individual control over personal information. We have an intrinsic say in what personal information is collected about us, how that information is subsequently used and how we can access or correct that information from data-collecting organisations.

Information privacy law provides a range of life-cycle protections that begin at the point of data collection and end with destruction or de-identification of no-longer-required data. In the interim, data collection organisations have a range of obligations to fulfil: the individual should be notified about the purposes of collection so that they can meaningfully consent to subsequent uses. Personal information can generally only be used for a defined purpose about which the individual is adequately informed. Individuals have a range of interaction mechanisms that seek to ensure the maintenance of control by giving them the ability to affirm the accuracy and currency of collected personal information. Personal information, once collected and stored, must be kept secure.

Despite the commonality of these types of protections, which originate from the same founding roots of principled application, different jurisdictions have different emphases about how information privacy law should apply. Two foundational issues are of importance: (1) the type of information that will trigger legislative or regulatory response and (2) the existence or absence of principled protections at the point of data collection. These issues are at the crux of significant variations between the jurisdictional approaches of the European Union (EU), the United States and the non-EU Organisation for Economic Co-operation and Development (OECD) countries such as Australia.

The ubiquitous collections of sensor data now unfolding in the collected world fundamentally challenge traditional information privacy protections. It is not legally clear whether, and in what forms, sensor data will be classified as the types of information that trigger information privacy law's application. Sensor data that can be collected from many sources can now be used to infer patterns and behaviours, thus obviating the need to collect personal or sensitive information directly from us. Moreover, the pervasive and continuous harvesting of all data trails challenges our conscious ability to rationally consent to the process of personal information collection.

The new norm of sensorised data collection processes, at the heart of developing smart business models, is also very different to the past collections of personal information that information privacy law is based upon. In the new forms of collections, we move from being active and autonomous participants who can control our own data to passive supplicants of infrastructures that are so unfathomable that the idea of individual control is nothing but an illusion. Instead of shaping our own destinies, we could instead be shaped by the many and multifarious organisations that collect, analyse and reuse our data.

To what extent does the collected world therefore require us to rethink the conceptual basis of control-based information privacy and its manifestation as the principled protections of information privacy law?

This book seeks to address that question. It argues that the collected world's new norms of sensor data collection are such that we need to reconsider the control basis of information privacy and its application in law. Several reasons are addressed.

The one-to-one, controllable data collection exchanges between individuals and data collectors are increasingly becoming a thing of the past. Collections from the sensorised spaces of the collected world, such as the smart home, involve multiple data collectors that collect sensor data from different sources and pathways. A new power context

emerges relating to the ability to coalesce data from smart environments, which are so fragmented that it is difficult for any one party to have control. Like the notions of the smart and collected worlds, the abilities of data collection and sense-making are intrinsically linked. This is recognised in information privacy law regarding limitations on primary uses and resultant secondary purposes. However, these limitations focus on the ability of an individual to retain control over their information as a right of input into the decision-making capacities of data-collecting organisations. Thus, information privacy law seeks to ameliorate power imbalances, but it does so in a way that no longer matches the accumulation and use of power in the sensorised environments of the collected world.

Fundamentally linked to the new processes of sensorised data collections are the underlying business models that contribute to the relentless push for truly ubiquitous collections. The drive is most clearly articulated in descriptions of big data analytics and the desire to collect everything to find insight through the unintuitive. While the force of the driver may have diminished somewhat, the after-effects are still palpable due to the norm of sensorised collections that continue to pervade. Sensor data can provide insight into historical patterns of activities, behaviours and personalities that can be used to predict and prescript future service outcomes. Value resides in the ability to locate, collect and analyse sensor data, which has now become the desired target for the new business models of the collected world.

In considering the new forms of sensor collection and business models, it becomes increasingly important to reconsider what control and autonomy means in the context of information privacy protections. It is arguable that control of personal information is no longer attainable in the sensorised environments of the collected world that have so many points of interaction across multiple parties. Even if it is attainable, it is questionable whether being able to control personal information provides the type of protection that is required. Individual control is more likely to operate effectively when there is a limit to the data that is generated and collected. However, it is questionable whether individual control is an effective measure in the face of ubiquitous collections of sensor data from complex, fractured and contested environments that are increasingly boundary-confused.

As a result, this book argues that both the concept of information privacy and its application in law need to be reconsidered because of the nature of the collected world. Section 1.2 reveals how this reconsideration unfolds throughout the book's three parts and nine substantive chapters.

1.2 The Book's Coverage

The book argues for a reformulation of information privacy's control basis to one that explicitly regards the new power consequences of the collected world. In so doing, Part I outlines the scope of the collected world. It examines developing business models, based on collections of sensor data, as a means of demonstrating the challenges that will arise for information privacy's control model and the application of principled protections of personal information exchange. Part II outlines the conceptual basis of information privacy and its expression as information privacy law. Part III then details the challenges to both the concept and the application of information privacy law that arise from the collected world, using the smart home coverage of Part I and the information privacy coverage of Part II. Next, in Part III, Julie Cohen's work is used in the reformulation of information privacy's new role of interrupting modulated power.[1] Part III's reformulation also provides a foundation for some areas of future information privacy law reform, specifically focusing on the type of information that triggers regulatory intervention and the need for a strong collection principle based on fairness. Throughout, the book's focus is on private sector data collectors rather than public, given the commercial drive for the collected world.

1.2.1 Part I: The Collected World

Part I examines the scope of the collected world, and it contends that the smart world is a collected world. The frame of the collected world is, by its very nature, broad. An understanding of conceptual breadth is necessary to fully consider the power consequences that unfold in

[1] Julie E Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (Yale University Press 2012); Julie E Cohen, 'What Privacy Is For' (2013) 126 Harvard Law Review 1904; Julie E Cohen, 'Between Truth and Power' in M Hildebrandt and Bibi van den Berg (eds), *Freedom and Property of Information: The Philosophy of Law Meets the Philosophy of Technology* (Routledge 2014); Julie E Cohen, 'The Networked Self in the Modulated Society' in Wouter de Been, Payal Arora and Mireille Hildebrandt (eds), *Crossroads in New Media, Identity and Law: The Shape of Diversity to Come* (Palgrave Macmillan 2015); Julie E Cohen, 'The Surveillance-Innovation Complex: The Irony of the Participatory Turn' in Darin Barney and others (eds), *The Participatory Condition in the Digital Age* (Minnesota University Press 2016); Julie E. Cohen, 'Affording Fundamental Rights: A Provocation Inspired by Mireille Hildebrandt' (2016) 4 Critical Analysis of Law 78; Julie E Cohen, 'The Biopolitical Public Domain: The Legal Construction of the Surveillance Economy' (2018) 31 Philosophy & Technology 213; Julie E Cohen, 'Turning Privacy Inside Out' (2019) 20 Theoretical Inquiries in Law 1; Julie E. Cohen, 'Review of Zuboff, Shoshana. 2019. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power' (2019) 17 Surveillance & Society 240.

the final chapters of the book, based on Cohen's modulation and her biopolitical domain. However, it is also necessary to consider the finer points of sensor data collection to clearly articulate the collected challenges that will arise for information privacy law. Thus, Part I uses the smart home as a collected-world case study to examine technological infrastructures, the effect of sensorisation and the business models that flow from the new data generation pathways of the collected world.

Chapter 2 begins the scoping discussion and provides an overview of technological development covering three areas – namely, smart individuals, smart buildings and smart environments. A key element of smartness across all these areas is sensorisation and the rapid spread of sensorised devices, which enables new forms of data collection. Focus is placed on the smartphone in its use as a sensor-collecting device that has individual, communal and societal purposes. Chapter 2 concludes by demonstrating the intractable link between the notions and benefits of smartness and what this actually entails in relation to data collection.

Chapter 3 examines the implications of sensorisation in a discrete, collected-world environment – the smart home. This venue is chosen as a collected-world case study for several reasons. First, the smart home is a site of dense sensorisation and thus a good space in which to explore technological infrastructures that underpin the smart world. Second, it is one of the prime sites of sensor data commercialisation, including by the new business models that are developing. Third, the home is a legally protected idyll of the 'private', and it plays a cherished role as a space of autonomous individual growth in liberal societies. The smart home therefore provides an appropriate site in which to consider the consequences of sensorisation, the business models that are unfolding and the impact these models have on both the concept and the application of information privacy law.

Chapter 3 details the complex data generation anatomy of the smart home and examines it from the standpoint of its sensing, reasoning and intervening processes. It does so from a multidisciplinary perspective involving legal, technical and sociological considerations. Even though the smart home is framed as a space of seamless technological experience, its infrastructural anatomy is fragmented and multifarious because it includes multiple data collection devices and diverse collection pathways. Chapter 3 concludes by highlighting that sensor data is key to the operation of the smart home and the business models that are now starting to develop.

Chapter 4 then examines in greater depth the commercial imperatives for collections of sensor data by exploring the rapid development

of smart home insurance business models. A brief history of smart home insurance is provided to situate three conceptualised models of smart home data exchange partnership involving insurers and smart home device or system providers – entitled Partnered Data Acquisition, Partnered Intermediary and Platform Entity models.

Each model involves a partnership arrangement between an established insurer and a smart home device or system provider. However, while each model seeks to capitalise value from smart home sensor data, the models do so in different ways, across three spectra – namely, *collection* of data, *connection* to mutually beneficial services and *condition setting*. An analysis of relevant privacy policies is undertaken to highlight each model's operational data structure, the sensor data collected and its foundational characteristics. In turn, this analysis highlights the commercial uses of smart home sensor data involving new logics, business relationships and intended service outcomes. Attention is given to the Platform Entity model specifically, as it harks to many of the power-related issues covered in Part III.

1.2.2 Part II: Information Privacy Law's Concepts and Application

Chapter 4's analysis of relevant privacy policies highlights some key differences in jurisdictional approaches to information privacy law and begins to give insight into some of the challenges to be faced in a collected world. Part II, in preparation for a critical examination of these challenges in Part III, details the conceptual bases of information privacy and its implementation in information privacy law. Part II examines what information privacy law seeks to protect and how it provides protections. On its face, this sounds like a straightforward task, but it is complex due to the many different purposes and emphases required of privacy and information privacy law.

It should already be growing apparent that the book adopts certain language and positioning about information privacy law and its relations to broader legal constructs of privacy. In this volume, 'information privacy' and 'data protection laws' are treated synonymously. However, the moniker 'information privacy' is preferred. The preference partly reflects jurisdictional bias, as it is the preferred referential mode in Australia, but it is also preferred because of its explicit acknowledgement of broader aspects of privacy. Information privacy is thus considered a constituent part of privacy law's wider conceptual family. In that regard, the book does not adopt a clean differentiation between information privacy law and privacy law in general, unlike the clearer delineation that is sometimes made between data protection and other

areas of privacy law.[2] Again, this is partly down to jurisdictional bias, but it also regards the conceptual examination of the book, which covers information privacy's role as a protector of purportedly autonomous spaces. Once in those conceptual spaces, it becomes more difficult to treat information privacy separately from its broader family.

With that in mind, Chapter 5 identifies, through coverage of key authors, four conceptual themes that underpin information privacy's development: (1) individual control over personal information, (2) informational access and personal autonomous growth, (3) a broader social and relational context and (4) privacy as a structural problem of power. Chapter 5 highlights that the control concept is dominant, as evident by its implementation as information privacy law. However, all themes become important to Part III's analysis, which uses Cohen's work to critique both the control and the autonomy themes as a basis for arguing for a stronger role for information privacy's relational context and power-related elements.

Chapter 6 identifies the different foundational structures and jurisdictional perspectives of information privacy law that involve EU, US and Australian legal frameworks. A historical perspective of information privacy law developments in each jurisdiction is provided based on three founding legal instruments for each jurisdiction. Historical development is important because it highlights that although jurisdictional laws are based on the same principled approach, different jurisdictions adopt different emphases. Two particular emphases are examined: (1) the type of regulated information that triggers regulatory response – namely, personally identifiable information in the United States, personal data in the EU and personal information in Australia – and (2) information privacy law's principled process of protection. Attention is given to collection principles as a means of outlining foundational differences between sectoral and comprehensive regimes of information privacy, particularly regarding the overt use of a notice-and-consent model.

1.2.3 Part III: Information Privacy Law for a Collected Future

Let's recap. Part II sets the conceptual and legal framework from which the collected-world consequences of Part I's analysis can be examined, particularly in relation to sensor data collections from the smart home. Part III then examines the consequences of the collected world and the challenges it will bring for information privacy law's dominant control

[2] See Gloria Gonzâlez Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer 2014) for an admirable example.

model and its manifestation in information privacy laws predicated on process protections. In doing so, Part III puts forward a reformulated role for information privacy law based on Cohen's work of the past decade, most notably on modulated power.

Chapter 7 returns to the smart home as a way of examining the collected-world challenges that will arise for information privacy law. It highlights that sensor data collections are different in nature to the type of data collections envisaged by the control model of information privacy. Smart home sensor data collections are circular and continuous, which challenges the basis of rationality modes of consent provision. Moreover, the very notion of control is challenged in boundary-dispersed environments, such as the smart home, which are essentially fragmented and contested. These factors give rise to significant challenges for the control model of information privacy law and its focus on the process of personal information exchange.

Chapter 8 then returns to the conceptual analysis of Chapter 5 to address what information privacy *should* protect in a collected world. A sustained critique of the control model is put forward in relation to five intended outcomes of information privacy law. Out of these five intended outcomes, two are broad in nature and reflect the conceptual intentions of information privacy. The first is the enhancement of individual autonomy through the creation of non-interference protections at the point of data collection to ensure unfettered decision making. The second regards the amelioration of power imbalances using power vacuums that preserve spaces for autonomous decision making.

Three narrower outcomes, focused on the application of information privacy law, then supplement the broader conceptual intentions. The first outcome reflects information privacy law's mode of transactional operation, which generally considers provisions of personal information as tradable exercises. The second outcome then regards the use of privacy policies, as information disclosure mechanisms, to ameliorate information asymmetries in transactional modes of operation. This outcome regards information privacy law's inbuilt balancing mechanism, which seeks to secure fair outcomes for individuals while ensuring that data exchanges flow for the benefit of data collection organisations and society.

Chapter 8 introduces Cohen's work as a means of further critiquing the control model and reshaping a conceptual focus of information privacy based on a more explicit, power-related role. The new focus sees a shift in what information privacy seeks to do and in doing so challenges some of the fundamental precepts of the control model and what information privacy currently seeks to protect. The five intended outcomes

of information privacy law thus change markedly and transit from protection of autonomy to situated inter-subjectivity, power vacuums to interruptions of modulation, transactional operation to boundary management, information asymmetries to social shaping and balancing mechanisms to exposing modulation.

At the heart of this reformulated movement is Cohen's work on modulated forms of power, which describes the consequences and challenges that arise from the collected world. Modulation offers a more complex frame through which to view the operation of power in the collected world, because Cohen considers power structurally across several different spectrums. These spectrums cover the broader political economy behind ever-cumulative forms of informational capitalism and its concomitant surveillant logics, infrastructural requirements and device designs – in other words, the use of modulated power flows from the macro structures of informational capitalism through to micro activities of sensorised data collections. This discussion therefore encapsulates many of the concerns raised in earlier parts of the book. More importantly, Cohen's work provides a platform that allows for new forms of information privacy law to develop that are explicitly designed for the power-related consequences of the collected world.

Chapter 9 examines how new forms of information privacy law could develop to interrupt modulated forms of power. It highlights some design points for future legal reform. The design points are not exhaustive, but they outline some key areas that would allow reforms to develop based on Cohen's principles of semantic discontinuity and operational accountability. The implementation of these principles would require some form of detachment from information privacy's core process protections, so that the law could apply in gaps and spaces at the outskirts of process. These gaps and spaces are important because, as Cohen argues, this is where selfhood flourishes and would therefore be a prime target for modulated forms of data collection. The design points would allow protection of gaps and spaces through the construction of new boundary options that create pauses in seamless forms of data collection and analysis. All of this would assist in information privacy law's new role in exposing modulation.

Chapter 9 also returns to Chapter 6's analysis and highlights the need for relational forms of regulated information and a collection principle based on fairness. The jurisdictional considerations introduced in Chapter 6 thus come to the fore. Chapter 9 contends that a greater focus on relational forms of personal information, such as personal data in the EU, would be an important interrupter of seamless application because it would have the effect of extending information privacy law's