The ethics of data privacy

by

Jeroen Seynhaeve

Thesis presented in fulfilment of the requirements for the degree of MPhil (Applied Ethics) in the Faculty of Arts and Social Sciences at Stellenbosch University

Supervisor: Prof Vasti Roodt

December 2022

Declaration

By submitting this thesis electronically, I declare that the entirety of the work contained therein is my own, original work, that I am the sole author thereof (save to the extent explicitly otherwise stated), that reproduction and publication thereof by Stellenbosch University will not infringe any third party rights and that I have not previously in its entirety or in part submitted it for obtaining any qualification.

December 2022

Dedication

I dedicate this thesis to my wife Ilse and our daughters Julie and Charlotte, who've stood with me during the countless hours of solitary writing, and who had my back when I caught a glimpse of the old Sisyphus. I also wish to thank my parents who have been supportive throughout my law and philosophy studies. I could not have wished for a better supervisor: Prof Roodt's guidance was gentle, helpful and intellectually stimulating. She not only skilfully managed to wrestle complex arguments out of me, but also planted the seeds for many of the ideas I present in this thesis. Much obliged!

Abstract

Technology, and in particular information and communication technology (ICT), often relies on sensitive data about people to deliver the results we want from them. There is nothing inherently wrong with this: our social, scientific, political and economic institutions and progress rely on this data, and would be seriously hampered if all data about people were considered private. However, recent technological advancements have led to a whole new relationship between people and ICT, and between ICT and privacy. As it turns out, access to vast amounts of personal data unlocks unprecedented possibilities. This has led to a plethora of new technologies that process all kinds of data about people, up to a point where our established notions of privacy struggle to keep up with technological advancements. This makes a recalibration of our relationship to technology, and in particular the role (data) privacy plays in this relationship, necessary and urgent. But before we can come up with new ways to manage privacy in relation to technology, we must first get clarity on what privacy is, and why it deserves protection. This is why this thesis starts with an overview of the current data privacy landscape and its different concepts and controversies, and with an argument for why this landscape is unprecedented. Chapters Two and Three juxtapose two different arguments for data privacy. The first claims that data privacy is justified in as far as it protects us against harm. I disagree with this claim, and argue that a harm-based approach to data privacy in a rapidly changing technological context is undermined by unreliable concepts and predictions of harm. The second argument, which I defend, claims that data privacy deserves protection because it constitutes a unique and necessary context for the protection of an underlying value: the fundamental principle of respect for persons. The method I propose for managing data privacy is derived from this second argument: rather than weighing up costs and benefits, we must deliberate moral values and practical concerns that are at stake when we evaluate data privacy dilemmas, and test the outcomes of our deliberations against the principle of respect for persons.

"The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the mass. His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man. Such a being, although sentient, is fungible; he is not an individual"

(Bloustein, 1964:188).

TABLE OF CONTENTS

INTRODUCTION

All societies have to balance privacy claims with other moral concerns. However, while some concern for privacy appears to be a common feature of social life, the definition, extent and moral justifications for privacy differ widely. Are there better and worse ways of conceptualising, justifying, and managing privacy? These are the questions that lie in the background of this thesis. My particular concern is with the ethical issues around privacy that are tied to the rise of new information and communication technologies (henceforth "ICT"). The focus here is on technologies involved in *processing* personal data in its broadest sense, including "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[1] The issue of moral concern is commonly designated as that of *data privacy*.

The first step is to consider why privacy matters, or ought to matter, in the first place. And here we run into our first difficulty, since both the conceptualisation of privacy and the justification for the right to privacy are matters for contention. On the one hand, we are animated by a moral concern for privacy in some sense; on the other, we lack the conceptual and moral resources for making sense of this concern or for promoting particular social policies and criticising others. This often-cited dichotomy (e.g. Thomson, 1975; Wasserstrom, 1978; Posner, 1978; Parent, 1983; MacKinnon, 1989; Schoeman, 1984; Allen, 2000; Solove, 2002 and 2015; Floridi, 2013) and its ensuing confusion have been the central motivation for most of the philosophical literature on privacy – including this thesis.

In what follows, I will suggest a way out of the confusion that pervades the current debate on data privacy. I will essentially argue two claims: one, that the *concept* of (data) privacy is uniquely characterised by a particular context within which we exchange information; two, that because (data) privacy constitutes an intrinsic *value*, its moral concerns and justifications

[1] Art. 4(2) of the European Union's General Data Protection Regulation 2016/679

ought to be deliberated as such. The first chapter sketches the current data privacy landscape by introducing a number of concepts and arguing the unique nature of the landscape. I argue that the traditional distinction between four kinds of privacy (physical, mental, decisional and informational) is no longer accurate, given the technological context that reduces, unifies and processes all aspects of people's lives by means of digital data. In fact, to hold on to the distinction leads to a fundamental misconception of data privacy. I further argue that today's distinction between data protection and data privacy runs the risk of ignoring the fact that the former is an inherent aspect of the latter. These arguments allow me to settle on a (provisional) definition of data privacy: controlling how data about identifiable people is processed by ICT. Next, I draw a line between descriptive and normative accounts of data privacy, and explain why this thesis belongs to the latter category. After a brief discussion of the coherence and distinctiveness theses, and of the difference between instrumental and intrinsic theories of privacy, I introduce the problem of data privacy as a distinct, coherent, and intrinsic moral concern. Three arguments support this position: one, data privacy is a *coherent* moral concern because it is motivated by a singular moral concept; two, data privacy is a *distinct* moral concern because the privacy challenges we face today are of a fundamentally new nature – distinct from any moral concerns we've faced in the past; and three, data privacy is an *intrinsic* moral concern that is predominantly justified, not by what it instrumentally protects us from, but by what it intrinsically constitutes.

Chapter Two makes the case against a harm-based, consequentialist approach to data privacy. After a brief introduction to the basic tenets of consequentialism I discuss harm-based arguments in favour as well as against privacy. I explain how privacy may protect us against psychological distress, but at the same time constitute the source of that distress; how privacy may be necessary for the proper functioning of democratic societies, but at the same time provide a cloak for anti-social and immoral behaviour; and how privacy protects us against the improper use of our personal data by others, but at the same enables us to conceal information or spread false information about ourselves in ways that are harmful to others. Next, I argue that consequentialism essentially relies on two flawed presumptions – that we *know* what harm is, and that we know how to *predict* it – and discuss the controversies surrounding definitions and predictions of harm. This argument becomes especially pertinent

in today's rapidly changing technological context: we may guess, and make assumptions, perhaps even find correlations, but don't really know or understand (yet) with any degree of certainty the harmful consequences today's data privacy violations are causing or will eventually cause – if any. I illustrate this with examples of recent data privacy violations, and with a brief overview of consequentialist arguments for and against data privacy. Those who invoke consequentialist arguments against data privacy claim that personal data is nothing more than a raw material that can be turned into something useful and valuable without harming anyone. Choosing to *move fast and break things* – a popular mantra that promotes the benefits of technological "permissionless innovation" over and above its risks and costs (Gilbert, 2021:164) – they draw our attention to the many benefits free data flows generate. Those who rely on consequentialist arguments in favour of data privacy, on the other hand, insist on actual and potential misuse of personal data. Rather careful than sorry, they draw our attention to the urgent need to take back control and protect ourselves against data privacy violations – precisely because we don't know which harm they may cause in the future. Others go one step further and argue that these violations are part of a broader ideology of power. What Chapter Two demonstrates is that vague definitions, unreliable predictions and inconclusive allegations of harm from both sides of the debate perpetuate a stalemate that fails to produce morally defensible answers to our growing data privacy concerns. Deliberating about data privacy from a consequentialist perspective is a dead end.

Chapter Three proposes an alternative to the harm-based approach, namely that privacy is an intrinsic value that deserves moral protection for its own sake. After a brief account of what I take values to be, and why we have a need to protect them, I introduce the foundational value of respect for persons, and lay out my main argument in two steps. The conceptual component of my argument returns to the definition of data privacy I had temporarily settled on in Chapter One, but now with the added consideration of the particular context, and particular circumstances and attitudes, within which information is exchanged. This addition is crucial, as it reveals the fundamental value that is at stake in our data privacy concerns, namely the inherent value of each and every person, which we protect by upholding an ethical principle commonly known as the principle of respect for persons. It is for this reason that the violation of privacy cannot (only) be expressed in terms of harm. I further argue that the principle of

respect for persons is consistent with, and in fact unthinkable without, some degree of privacy. I reply to potential challenges to a value-based approach to data privacy by showing that (i) values and value trade-offs are fundamentally different from consequential benefits and cost-benefit analyses; (ii) the suspension of one value in favour of another is not inherently contradictory; what matters is morally defensible deliberation about values and valid individual consent; (iii) data privacy concerns cannot be reduced to other moral concerns and therefore deserve a specific, distinct protection.

Finally, because this is a book in applied ethics, I attempt an answer to the question as to how we ought to apply a value-based approach to practical data privacy concerns. I argue that a revised, three-pronged version of John Rawls' reflective equilibrium, founded on the non-negotiable principle of respect for persons, is the best possible procedure to deliberate data privacy concerns in relation to other moral values.

1. DATA PRIVACY: SITUATING THE PROBLEM

1.1. Introduction

This thesis deals with three questions: *what* is data privacy, *why* should we protect it – or conversely, reject it – and *how* should we manage it? The answers to these questions are related and often overlapping: the justification for why and how we should manage the right to data privacy largely depends on how we define the concepts that constitute data privacy, and vice versa. I therefore start with a critical analysis of the concepts of privacy, data privacy, data, and information, and argue that (i) data privacy should not be reduced to informational privacy or to data protection, and (ii) it is a mistake to exclude allegedly anonymous or de-identified data from our data privacy concerns. This discussion allows me to settle on a provisional definition: data privacy refers to measures and tools that aim to control how data about identifiable people is processed by ICT. Next, I discuss distinct types of ethical theories of privacy that have been proposed in the philosophical literature. One distinguishes between theories that argue that privacy is motivated by coherent moral concerns on the one hand, and theories that argue that privacy is motivated by a cluster of disjointed concerns on the other. Another distinguishes theories that argue that privacy is characterised by distinct moral concerns versus theories that claim that privacy concerns may be reduced to other concerns. A third distinction separates theories that justify privacy on the basis of its intrinsic value from theories that posit that privacy is merely instrumental. Finally, because this is a thesis on *data* privacy, I discuss the relationship between privacy and technology. By means of a brief overview of Luciano Floridi's concept of the Information Society and his account of third-order technologies, I argue that new ICTs pose entirely new challenges to established notions of privacy, which necessitates an urgent and all-encompassing moral evaluation of data privacy. I will therefore conclude that data privacy is a distinct and coherent moral value that intrinsically deserves protection. To be clear, what follows is a discussion of largely analytical concepts. Nevertheless, these concepts are a useful way of making sense of the conceptual and moral landscape of the current debate around data privacy.

1.2. Privacy as a moral concept

1.2.1. Conceptualisation versus justification

An ethical evaluation of data privacy – the subject of this thesis – approaches concerns around data privacy from a normative perspective: it aims to argue morally defensible justifications for why we *ought to* recognise, promote, and protect, or conversely reject, data privacy. It tries to formulate an answer as to why people should have a right to control personal data about themselves. Do people have good reasons for keeping certain information private? And why should we, as a society, protect a right to data privacy?

However, all too often, moral discussions around data privacy are confounded by the lack of clearly defined concepts – so vague that they are "practically useless" (Solove, 2015:73) or perhaps even a "haystack in a hurricane" (Bloustein, 1964, in Schoeman, 1984:156). If we want these discussions to stand a chance of producing morally defensible answers, we must first have clarity on the basic concepts that underlie our data privacy concerns: data, information, privacy, and data privacy. We may start this conceptual analysis from a descriptive perspective, and look at established privacy practices (Gert and Gert, 2020). Anthropological studies, for example, suggest that whereas a concern for privacy may be a natural, inherently human, or at the very least universally shared concern, its definition, extent and moral justifications differ across times and cultures (Westin, 1967:56, 61 and 67; Kasper, 2007:185; Murphy, 1964:51). More recently, the rise and ubiquity of new technological possibilities for processing digital data containing sensitive personal information about people, has made data privacy a topic of academic study in the fields of law, computer science, data science, and statistics (Torra and Navarro-Arribas, 2014). For our purposes, however, one particular data privacy practice deserves a closer look: the globally emerging practice of regulating the processing of personal data. In what follows, I will focus on two of these regulations: the European Union's *General Data Protection Regulation*[2] (henceforth "GDPR") and South Africa's *Protection of Personal Information Act*[3] (henceforth "POPIA").

[2] The General Data Protection Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC

[3] The Protection of Personal Information Act, No 4 of 2013

Data privacy is often mistakenly understood as a digital version of *informational* privacy, and distinguished from other kinds of privacy on the basis of what they aim to protect – physical, mental, and decisional privacy (Floridi, 2014:102). Physical privacy aims to protect our bodies and sensory experiences against nonconsensual intrusions and manipulations, whereas mental and decisional privacy protects the autonomy and freedom of what goes on in our minds. This view implies that informational privacy provides a separate kind of protection – protection of *information* that relates to the three other kinds of privacy, by giving us control over who has access to, and what can be done with that information. Others argue that data *protection* is a right on its own, distinct from the right to privacy. The European Union, for example – globally recognised for its pioneering role in data privacy protection – kicks off its GDPR with the declaration that the protection of personal data is a separate fundamental right (Recital 1). In fact, even though the fundamental rights to a private life and associated freedoms[4] are said to underlie the right to data privacy (Ustaran, 2019:4), the GDPR does not mention the word *privacy* once.

However, there are a number of problems with views that distinguish different kinds of privacy, or that disconnect data protection from the fundamental right to privacy. By separating different kinds of privacy, the first view ignores the interdependence of the protection of different aspects of our lives we seek through a right to privacy: privacy as a right to nondisclosure, and privacy as a right to noninterference – or the "right to hide and the right to decide" (Gersen, 2022:25). In other words, this view ignores the intrinsic relationship between informational privacy and the other kinds of privacy: how we protect personal information often has an impact on how we protect a person's physical, mental, and decisional autonomy, and how we define the latter determines which information deserves protection. But while one may point out in reply that these distinctions are intended to be merely analytical, they tend to lead to a fundamental misconception of data privacy in the context of today's data-driven and technology-powered society. The conceptual distinction between different kinds of privacy ignores the fact that our bodily interactions, mental processes, autonomous decisions, and personal identities are increasingly defined by digital data about

[4] Articles 12 and 19 of the Universal Declaration of Human Rights, 1948, and Articles 8 and 10 of the European Convention of Human Rights, 1950

us, and by how technologies process that data. Data privacy, therefore, is not just a digital version of an isolated kind of (informational) privacy, but includes, and cannot be distinguished from, all other kinds of privacy notions that aim to protect essential aspects of identity, integrity, freedom and autonomy of persons in a society dominated by data.

Perhaps there are good reasons to accept the second view: separating data protection from the right to privacy avoids the controversies that generally dominate discussions around privacy. But avoiding controversies is not an argument for treating data protection as a separate concern. Rather, in particular in the context of current data-powered technologies, data security is part of a broader set of data privacy concerns (Solove, 2015:73). South Africa, for example, introduces POPIA with the recognition that the Constitutional right to privacy "includes a right to protection against the unlawful collection, retention, dissemination and use of personal information" (Preamble). I will therefore be using the term *data privacy* throughout this thesis – rather than data protection – in recognition of the fact that the protection of personal data is not separate from, but an inherent aspect of our moral conceptions of and justifications for privacy.

We find support for this broad interpretation of data privacy in current legal definitions. The central concept of data privacy – personal data – is kept "intentionally broad" (Ustaran, 2019:73) to allow it to apply to changing circumstances, including the invention of new technologies. That is why data privacy regulations, such as the GDPR and POPIA, are "principle-based" (de Stadler, Luttig Hattingh, Esselaar, Boast, 2021:44). Rather than providing an exhaustive list of the specific types of information that are covered by their protection, data privacy regulations rely on an open-ended definition of personal data: personal data means *any information* by which a *person*[5] can be directly or indirectly *identified* – regardless of what the information reveals about that person. In other words, the essential characteristic of personal data is not what it contains but what can be done with it. Thus we see that, while some regulations like POPIA, cite an (non-exhaustive) list of examples of what may contain personal data (Sections 1 and 26), others like the GDPR, provide no such list, but merely specify that personal data is characterised by its capacity to

[5] Both GDPR (Recital 27) and POPIA (Section 1) exclude deceased persons from their protection

identify a person by reference to their name, an identification number, location data, an online identifier or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity (Art 4(1) GDPR).

By focusing on the instrumental significance of personal data, these definitions aim to draw a line between two different concepts that are often used interchangeably: *data* and *information* (ibid:19).[6] Data is a set of raw facts, usually represented by numbers or codes that are meaningless in themselves. Information, on the other hand, is data that has been structured, linked, and aggregated into a concept that enables us to interpret, understand and use these facts within a meaningful context. For example, while raw data may look something like 278614-2-49, its informational counterpart would look something like: unique identifier = 278614, gender = 2, age = 49. Data privacy aims to protect data in as far as this data relates to persons – not raw, anonymous, and meaningless data. However, the line between data and information is not drawn that easily. Crucial in the discussion of data privacy is the question as to when data constitutes information – and more particularly information that makes the identification of persons possible. While legislation on data privacy has adopted the broadest possible approach by protecting *any* data that can or could identify persons *directly* or *indirectly*[7], *now* or in a reasonably foreseeable technological *future*,[8] the problems of *de-identification* or *pseudonymisation*, *anonymisation* and *re-identification* remain. *Anonymous* data is data that "does not relate to an identified or identifiable natural person" or that has been "rendered anonymous in such a manner that the data subject is not or no longer identifiable" (Recital 26, GDPR). *Coded* data is identifiable, private data that is represented by a unique identifier (e.g. patient 27). While all of these so-called privacy-protective measures aim to disconnect data sets from personal identifiers, de-identification stores these (usually encrypted) connections in separate records, which still leaves the data vulnerable to unauthorised access to the unique encryption key. Therefore, truly de-identified data would imply that the connection with its personal identifier has been destroyed. Then again, data which in itself appears anonymous may turn out to be able to identify persons when

[6] For example, the GDPR refers to "personal data", while POPIA refers to "personal information"

[7] Art 4(1) and GDPR

[8] Section 1 POPIA

aggregated with other data, or by means of future technology.[9] I therefore disagree with the claim that the term 'personal data' is a misnomer (de Stadler, Luttig Hattingh, Esselaar, Boast, 2021:19). Data privacy not only protects persons from being identified by means of meaningful personal information, but also protects persons from being identified by means of raw data in as far as it can be shown that this data can be used now, or in a technologically foreseeable future, to identify persons. In line with this generally adopted approach that aims to protect *any data* that may possibly identify persons – even data that appears to be meaningless today – I will be using the term 'personal data' throughout this thesis, and settle on the following working definition of data privacy for now: data privacy refers to measures and tools that aim to control how data about identifiable people is processed by ICT.

1.2.2. The coherence and distinctiveness theses

Ferdinand Schoeman identifies two general positions in the philosophical debate on privacy. The *coherence thesis* argues that all privacy issues are unified by a single, coherent moral concern. The *distinctiveness thesis* holds that privacy is a distinct moral concern, distinguishable from other moral concerns (Schoeman, 1984:14 and 22). The different theses are not necessarily mutually exclusive. A theory of privacy may claim that privacy concerns are unified by one single, coherent and distinct concern, or by an incoherent cluster of distinct concerns, or by concerns that are shared with (or may even be reduced to) other concerns.

There are many examples of coherent and distinct theories of privacy. While some argue that privacy is necessary to cultivate virtue (Aristotle, in Swanson, 1992) and to protect the autonomy and liberty of persons against the interference of others and the state (Bloustein, 1964; Gerstein, 1978; Reiman, 1976; DeBrabander, 2020:78-88), including our intimate interpersonal relationships (Fried, 1968; Rachels, 1975), others argue that privacy is a social good (Magi, 2011:205; Kasper, 2007:186), and necessary for the proper functioning of liberal democracies (e.g. Benn, 1971; Courtland, Gaus, and Schmidtz, 2022; Habibi, 1996:90; Habermas, 1998:417). And whereas some argue in favour of privacy to protect a right to be let

[9] I discuss examples of the first in Chapter Two (Rocher, Hendrickx and de Montjoye, 2019; de Montjoye, Hidalgo, Verleysen, et al., 2013). For a discussion of the problems: https://iapp.org/news/a/de-identification-vs-anonymization/

alone and shielded from mental distress (Warren and Brandeis, 1890:205; the Stoics, in DeBrabander, 2020:78-82), or to protect a zone of special interests (Scanlon, 1975:315) or specifically private areas (Benn, 1971:236), others argue against privacy on the basis that it perpetuates irrelevant social norms (Wasserstrom, 1978), or enables social and economic inequalities and abuse (Allen, 2000:1177; MacKinnon, 1989:116, 191; Posner, 1978).

A number of authors either rejects the coherence thesis, or the distinctiveness thesis, or both. Those who reject both argue that every account of privacy thus far has been "either too narrow or too broad" (Solove, 2002:1126 and 1094). The search for a single, overarching conception and justification of privacy is a fool's errand. Perhaps privacy is an example of Wittgenstein's claim that not all concepts have a common denominator, core or essence (ibid:1099). Others argue that theories of privacy are generally characterised by disarray and contradictions (Parent, 1983:341) and that this gives us good reasons to puzzle over the significance of privacy, and for "being suspicious of its value" (Schoeman, 1984:1). Rather than shedding light on our moral concerns around privacy, most theories of privacy seem to have done little more than confounding the various issues at stake with deeply challenging and contradictory claims (Parent, 1983:341). Another claim is that existing notions of privacy have not yet caught up with the challenges of new technologies (Green and Shariff, 2021), and that we would be naïve to expect our privacy concerns to be the same as before (Floridi, 2013:236).

One commonly accepted view is that privacy is a distinct moral concern that is itself made up of an incoherent cluster of concerns, or "freedoms from" (Floridi, 2014:102). William Prosser, for example, defends the distinctiveness thesis but rejects the coherence thesis by arguing that privacy concerns are motivated by different interests – that is, the need for protection against invasion of a person's private affairs and conduct, against the publication of private or false information, and against taking advantage a person's private information (Prosser, 1960:107). I have argued earlier why a view that distinguishes different kinds of privacy is conceptually mistaken – in particular in the context of today's data-driven society.

Judith Jarvis Thomson famously rejects both the coherence thesis and the distinctiveness thesis and argues, instead, for a "simplifying hypothesis" (Thomson, 1975:306). In Thomson's view, trying to protect privacy concerns by means of a distinct right to privacy unnecessarily complicates matters. The right to privacy is redundant because privacy concerns are simply derived from other, well-established concerns. Firstly, the right to privacy is not one, coherent right, but rather a cluster of rights. Secondly, this cluster of rights is not distinct from, but intersects with other clusters of rights, most notably those that reflect the right over the person and property rights (ibid:306). According to Thomson, it is perfectly possible to explain the moral concerns we wish to protect by a so-called right to privacy by means of these other rights. For example, we don't need a concept of privacy to protect personal data. First of all, information about a person is made up of facts. You don't violate a person's rights by simply knowing certain facts about them. Nobody can claim ownership over facts, so it doesn't make sense to try and claim ownership by means of an ill-defined right to privacy. Secondly, if we want to protect ourselves against people that try to get access to information about us, we can do this perfectly well on the basis of the right over one's person and individual property rights. To eavesdrop, for example, is nothing more than making inappropriate use of information that another person owns. If we want to protect personal data, we can perfectly do so on the grounds of a person's property rights, and demand that certain actions that may be taken to get hold of information, are prohibited (ibid:307). Again, this demand has nothing to do with the protection of some vague concept of privacy, but with the clearly defined protection of individual property. Most privacy theorists, however, have tried to refute Thomson's arguments by demonstrating what makes privacy concerns distinct and coherent.

1.2.3. The instrumental versus intrinsic value of privacy

A summary overview of privacy theories reveals another distinction – this time, between instrumental and intrinsic theories of privacy. An instrumental theory in favour of privacy justifies the right to privacy on the basis of its instrumental value, which is generally expressed in terms of the role it plays in *protecting* people and their personal interests against a "morally harsh" and "insufficiently understanding, benevolent, respecting, trustworthy, or caring" world (Schoeman, 1984:403). However, an instrumental theory may equally be invoked against privacy, by arguing that privacy ought to be rejected precisely because it

enables and perpetuates irrelevant social norms and wrongful social behaviour (Wasserstrom, 1978; Allen, 2000; MacKinnon, 1989; Posner, 1978). An intrinsic theory of privacy, on the other hand, argues in defence of privacy independent of its instrumental role. It seeks to justify privacy on the basis of its intrinsic value – of what it *constitutes* and *enables*. Privacy, most intrinsic theories of privacy argue, set out the necessary conditions for persons to be persons. Privacy is essential with respect to the "multidimensionality of persons" and with respect to the "personal or inner lives of people" (Schoeman, 1984:416). It is a necessary condition, an inherent characteristic, for the development and management of our free and autonomous personalities, intimate relationships and life projects.

1.3. Privacy and technology

Historically, there has been a "strong relationship between privacy and the development of technology" (Holvast, 2009:13). The new "mechanical devices" the popular press had at its disposal – more specifically the advancement of photography and printing technologies – play a central role in what is commonly considered a seminal essay on privacy (Warren and Brandeis, 1890:195). Charles Fried, too, writes about the privacy implications of a *hypothetical* device that would monitor a person's location, medical data, alcoholic blood content, conversations and brain waves, and invokes technological progress as one of the reasons why a moral discourse on privacy is urgent (Fried, 1968:203). Alan Westin and Richard Wasserstrom specifically point out the unique technological possibilities for invading privacy (Wasserstrom, 1978:317; Westin, 1967:71). Thomas Scanlon raises the inadequacies of existing privacy conventions in the face of new technologies (Scanlon, 1975:321), and Edward Bloustein adds the significant need for analysis of privacy interests in reply to scientific and technological advances (Bloustein, 1964, in Schoeman, 1984:157). Adam Moore writes about the "age of transparency" and quotes Brin, Sykes and Rosen to proclaim that privacy is threatened by the proliferation of information technology and computing (Moore, 2012). The contemporary Oxford philosopher Luciano Floridi argues that privacy is a function of forces that shape, oppose and promote flows of information, and that this *informational friction* is largely determined by technology (Floridi, 2014:105). Shannon Vallor argues that technologies have always shaped our moral practices, because throughout history they have enabled and restricted how we think, act and value (Vallor, 2016:2). And the

view that "Rapid technological developments and globalisation have brought new challenges for the protection of personal data"[10] underpins the world's leading data privacy regulations.

But while the relationship between privacy and technology is widely accepted, there is disagreement on the nature of the challenges new ICTs pose to established notions of privacy. Some claim that these challenges are not different from privacy challenges we have faced in the past, while others argue that the current technological transformation of our world implies privacy challenges of a different, entirely new nature. Because the way in which we respond to this question determines how we (should) manage data privacy in the current technological context, I will briefly discuss one answer, and argue in favour of another in the section that follows.

1.3.1. More of the same

Some argue that there is nothing new about today's privacy challenges – apart from the fact that there are just more of them. Accepting that technology has an impact on privacy does not necessarily mean that an increase of technological innovation changes the nature of this impact. Those who argue that today's privacy challenges only differ in degree, not in kind, find support in the widely and intuitively accepted *2P2Q*[11] *hypothesis* of a *continuist* philosophy of technology. The 2P2Q hypothesis explains today's privacy challenges as a mere continuation of old problems. The moral challenges today's technologies pose are simply more of the same – quantitatively *more* because the degrees of processing and pace have increased spectacularly, but qualitatively the *same* because the challenges are no different from challenges in the past (Floridi, 2013:230). I disagree with this view. In the rest of this section, I will show that a *continuist* philosophy of technology fails to grasp and respond to the new nature of privacy challenges. The world has changed fundamentally. Rapid and ubiquitous technological progress has created a "global information society enabled by a massive electronic communications network of unprecedented bandwidth and computing power" (Vallor, 2016:5). As a result, we are faced with *more* privacy challenges on a *wider scale*. But more importantly, we are faced with challenges of a *different nature*, too.

[10] Recital 6 GDPR

[11] Processing, speed (or Pace), Quantity and Quality

1.3.2. The Information Society

New ICTs have fundamentally changed how we shape and live our personal and social lives. In particular our new relationship with technology, and the emergence of new kinds of technologies that independently interact with other technologies, have created an unprecedented, data- and technology-driven world. I will explain these new relationships below, but before I do so, consider the following statistics that illustrate the impact of these new relationships and technologies on (personal) data. From 1946[12] a historical trend that is commonly known as Moore's law indicates that computing power has doubled (and will continue to double) about every two years. The number of personal computers in use worldwide rose from 48,000 in 1977 to 125 million in 2001, 500 million in 2002 to one billion in 2008 – a number that is estimated to increase annually by 12%.[13] Households with access to a computer rose worldwide from 27% in 2005 to 47% in 2019 – for developed countries, this number is closer to 80 percent.[14] The number of smartphone subscriptions worldwide nearly doubled between 2016 and 2022, and is expected to rise to almost 8 billion in 2027.[15] The International Data Corporation predicts that the Global Datasphere – a measure of all new data that is captured, created, and replicated in any given year across the globe – will grow from 33 Zettabytes in 2018 to 175 Zettabytes by 2025 (Reinsel, Gantz and Rydning, 2018:3). This growth is not only reflected in the quantity (volume) of the data, but also in its unique characteristics: veracity, validity, volatility, and value. These characteristics make so-called *big data* uniquely suitable for the algorithmic processing on which new technologies rely, in ways that one can interact with and learn from another, to a point that defies human cognition (Leonelli, 2020).

Luciano Floridi has developed a terminology that helps us to conceptualise this new world. He uses the term *hyperhistory* to indicate this new point in history at which humanity is

---

[12] The year commonly taken as the start of personal computing, with the launch of ENIAC (Electronic Numerical Integrator and Computer), the first programmable, electronic, general-purpose digital computer made in 1945

[13] en.wikipedia.org/wiki/History_of_personal_computers#Market_size

[14] statista.com/statistics/748551/worldwide-households-with-computer/

[15] statista.com/statistics/330695/number-of-smartphone-users-worldwide/

establishing fundamentally new, hyperconnected relationships with technology, and *infosphere* to describe the "informational environment constituted by all informational entities, their properties, interactions, processes, and mutual relations" (Floridi, 2014:41). People interact in the infosphere as *inforgs:* "informational organisms, mutually connected and embedded in [the infosphere] which we share with other informational agents, both natural and artificial, that also process information logically and autonomously" (Floridi, 2014:94). In the context of this new hyperconnected reality, the old distinction between offline and online reality has blurred into a single *onlife* reality, a consequence of "the blurring of the distinction between reality and virtuality" and "the blurring of the distinctions between human, machine and nature" (Floridi, 2015:7). Where ICTs used to operate within the limits of specifically designed three-dimensional environments (*envelopes*) outside of which they had no way of operating, *hyperhistorical* societies are turning the entire world into this kind of environment: the whole world is turning into one big *envelope* in which ICTs are operating at an optimal level. "Nowadays, enveloping the environment into an ICT-friendly infosphere has started pervading all aspects of reality and is visible everywhere, on a daily basis" (Floridi, 2014:144).

The concepts that Floridi has introduced allow us to gain a better understanding of this new world. His analysis reflects what is known as the *Theory of Technological Determinism*: the belief that societies are ultimately defined by the technologies that shape them (Hauer, 2017). The theory has been argued in various forms by philosophers as diverse as Martin Heidegger (Blitz, 2014) and Karl Marx (Bimber, 1990). Central to Floridi's analysis is his concept of the 'Information Society'. We may label any society in which people exchange various kinds of information an *information society*, but this is not what he has in mind when he introduces the concept. The contemporary Information Society differs from all previous social contexts in so far as it involves a fundamental shift in the relationship between people and technology (Floridi, 2014:26).

We may explain this shift as follows. First-order technologies solve a human need or extend human natural capabilities: the axe as an extension of our hands, writing as an extension of our memories, the wheel as an extension of our movements, and the telephone as an extension

of our voice. Floridi locates these first-order technologies between humans and natural *prompters* – for example, the sunhat is technology between the hiker (human) and the sun (natural prompter), or the saddle is technology between the rider and the horse. Second-order technologies, on the other hand, are no longer located between people and natural prompters, but between people and *technological prompters*. A screwdriver, for example, is technology between a human and a screw – a prompter which is in itself also a piece of technology, as are locks and engines (ibid:27). Today's technological development, however, is characterised by the "revolutionary leap" to third-order technology in which prompters as well as users are technological (ibid:29). To put this differently, the relationship between humans, technologies and prompters changes fundamentally and exponentially when technology is no longer developed by humans in response to natural or technological prompters, but by the ability of technology to interact with other technologies. The fundamental shift of our role and position in this is crucial. "We, who were the users, are no longer in the loop" (ibid:30). As a result, the Information Society is essentially constituted by, optimised for and fundamentally reliant on technologies that themselves rely on other technologies and on large and unhindered volumes of data – including personal data about people.

1.3.3. Privacy challenges of a new nature

The implications of Floridi's analysis are far-reaching for our moral evaluation of data privacy. If the nature of our relationship with technologies has fundamentally changed, then surely so have the privacy challenges these technologies pose to our personal data. Moreover, today's privacy concerns form part of a broader set of moral concerns which did not apply to previous privacy concerns. What is the place and role of human morality in a world defined by data and technology? The continuist 2P2Q hypothesis does not account for this fundamental shift and these new moral challenges. It is a shift of *ontological* proportions (Floridi, 2013:228) in that it changes "the very nature of the infosphere, that is, of the [informational] environment itself, of the [informational] agents embedded in it and of their interactions" (ibid 206).

The Information Society reduces people to *packets of information* or *information micro-environments* (ibid:259) – digital profiles that are continuously optimised for data processing.

This directly affects people in three ways. Firstly, new ICTs are by design *Privacy Intruding Technologies* (Floridi, 2013:236) – designed to collect, store and process more, not less, of personal data, because they fundamentally rely on this data to operate, learn and develop. It would seem then that privacy violations are built into these technologies' design, and that protection against these violations essentially restricts technologies from optimally doing their job. Secondly, more and more important and invasive decisions about people are being made on the basis of the available data, and this data only. In other words, not only are persons viewed as packets of information, these packets are also the definitive source of information about them. It is assumed that the data is never wrong – not even when the person the data relates to, objects. Thirdly, a violation of data privacy has implications of an unprecedented nature for the person the data relates to. If data privacy violations used to be violations of particular information about a person, today data privacy is "nothing less than the defence of the personal integrity of a packet of information" and a privacy violation is "an infringement of her me-hood and a disruption of the information environment that it constitutes". In other words, a data privacy violation has the potential to affect not only some aspects of a person, but *all* of her personhood in as far as that personhood is constituted by data. Floridi makes this point succinctly: violations of data privacy no longer merely constitute theft or trespassing of particular information about a person, but involve the "kidnapping" of the entire identity of that person (Floridi, 2014:114).

A statement from the biologist Edward Osborne Wilson, when applied to data privacy, captures the essence of the new moral landscape and challenges: "What Is Human Nature? Paleolithic Emotions, Medieval Institutions, God-Like Technology" (Wilson, 2017). Privacy concerns are part of, and must be evaluated in the context of, a new world that is characterised by a new kind of relationship between humans and technology: people with hard-wired palaeolithic emotions and cognitive capacities, who organise themselves and their societies in medieval institutions, are being targeted by God-like technologies. Shannon Vallor, too, argues that the 21st century has taken the historical relationship between technology and morality to entirely new levels, and that our moral choices today must therefore be "technomoral choices" because our moral challenges are directly determined by what new technologies make possible (Vallor, 2016:2). Part of what these new technologies make

possible, seem to be in direct conflict with established notions of privacy. Comparing small town gossip with the commercialisation of new media gossip, Edward Bloustein makes the following observations. Small town gossip has a social role to play, is interpersonal with a human touch, takes place between mutually interdependent people in similar power positions that often love or sympathise with one another, does not affect human pride and dignity, can be easily mitigated and corrected, and in fact is often not believed or only grudgingly and surreptitiously believed. Privacy violations committed by mass media outlets, on the other hand, are motivated by cold, commercial interests, and are impersonal and unilaterally damaging, hard to retract or correct, published far and wide among people unrelated to the subject of the violation, and treated as true and authentic (Bloustein, 1964:173). Twenty-first century ICTs have taken Bloustein's observations to entirely new levels, and have enabled privacy violations for entirely new purposes: large-scale social, political and economic *manipulation*. The unique combination of global access to data about people on the one hand, and the surgical (some say *military*) precision of its computational processing on the other hand, makes possible the "gradual, slight, imperceptible change in people's behaviour and perception" (Jaron Lanier in *The Social Dilemma*, 2020). While privacy rights may have been violated in the past for reasons of surveillance, public health and security, or for commercial, political and social reasons, *micro-targeted manipulation* is a new addition, enabled by new technologies' capabilities to collect, aggregate, interpret and apply large amounts of data about people that personally resonates with them. This has given rise to a whole new industry of data brokers[16] that trade (often very sensitive) personal data with companies, governments, and criminals for all kinds of purposes, but mainly to "sell the power to influence you" and the "power to predict your behaviour" (Véliz, 2020:21 and 49).[17] It is a concern that plays a central role in Shoshana Zuboff's concept of "surveillance capitalism" (Zuboff, 2019) – "the unilateral claiming of private human experience as free raw material for translation into behavioural data" (Zuboff, 2019). Luciano Floridi, too, is unambiguous when he announces

[16] The global data broker market was valued at US$232.634 billion in 2019 and is expected to grow at a rate of 5.80% over the forecast period to reach US$345.153 billion in 2026 (knowledge-sourcing.com/report/global-data-broker-market)

[17] It is expected that total advertising-spend will reach $706bn in 2022 (up from $634bn in 2019), of which digital advertising accounts for 62% of the total (zenithmedia.com/digital-advertising-to-exceed-60-of-global-adspend-in-2022/)

the *Fourth Revolution*. After humanity had to accept that we are not the centre of the universe (Copernicus), not the centre of evolution (Darwin) and not the centre of our mental lives (Freud), we now have to accept that we are not at the centre of intelligence (Floridi, 2014:3).

1.4. Conclusion

This chapter has attempted to shed a light on the most important concepts that underpin current moral concerns around data privacy: privacy, data, and technology. By critically analysing these concepts and their relations, and arguing in favour of particular definitions while rejecting others, I hope to have provided the conceptual clarity we need to embark on a normative analysis in the chapters that follow. Crucially, I have shown that data privacy in the present technological context is characterised by the following: (i) it covers any data that may be traced back to an identifiable person, and (ii) its protection is challenged in ways we have never dealt with before. This leads me to posit claims that I intend to argue in the next chapters. Firstly, data privacy is a coherent moral concern because it is motivated by a singular moral issue: the control we want over data that may reveal information about us, and the concerns we have around this data falling into the wrong hands, for the wrong reasons. Secondly, data privacy is a distinct moral concern because we cannot rely on other moral concepts to manage its protection – doing so would leave out aspects that we deem crucial to our notion of privacy. And finally, data privacy intrinsically deserves protection because its value does not merely rely on the role it plays in protecting other interests, but its value is inherently constitutive for protecting persons qua persons: a person simply stops being a person without it. The definition of data privacy I have settled on for now is provisional – it only covers the instrumental role of data privacy, but does not yet identify its moral justification. An instrumental definition of data privacy only tells us what it aims to do (to protect identifiable people) but does not yet provide a justification for why people deserve this protection. The latter may be approached from two perspectives: one, data privacy is instrumentally valuable as a safeguard against harm, or two, data privacy is an intrinsic value which ought to be protected for its own sake. Chapter Two examines the first approach and shows why it fails. This sets the scene for the argument in favour of data privacy as an intrinsic value in Chapter Three.

2. ARGUMENTS AGAINST A HARM-BASED APPROACH

2.1. Introduction

Much of the current debate about and regulation of data privacy focuses on the harmful consequences of data privacy violations. This should not be surprising, as we will see that a great deal of ethical theories of privacy rely on psychological, sociological, and proprietary harm to argue for or against privacy protection. However, there are two fundamental problems with an approach to data privacy that focuses solely on harm in the context of rapidly changing technology. First, it assumes that we know, and can agree on, what would constitute harm in this context. However, a critical analysis of harm theories reveals a recurring problem: all theories of harm struggle to define the perspective from which harm ought to be defined: is harm an individual qualification, or are there universal parameters by which we may determine harm? The question is particularly pertinent in the current context that presumes everyone's individual responsibility for the personal data they share with ICT. Second, a harm-based approach to data privacy assumes that we are able to predict harmful consequences with any degree of certainty. But this raises three important ethical questions. How can we possibly know all the consequences of our actions? Are we responsible for harm we have not predicted, or of which we are not even aware at the time of our action? And to what extent should we be allowed to risk harmful consequences in the absence of certainty? In reply, I will argue that concepts and predictions of harm are fundamentally ill-founded, or at least unreliable. But even if one disagrees with my general arguments against a harm-based approach to data privacy, I will also argue that consequentialism is particularly inadequate to manage data privacy concerns in the particular context of the Information Society. Most importantly, a brief overview of the current debate around data privacy demonstrates that vague definitions, unreliable predictions and inconclusive correlations of harm from both sides of the debate perpetuate a stalemate that fails to produce morally defensible answers to our growing data privacy concerns.

2.2. Harm-based arguments

2.2.1. Consequentialism

While hardly any ethicist today would defend an isolated, top-down application of any ethical theory, uncovering the moral concepts and reasoning that motivate our practical judgements is still helpful to make sense of them. In its simplest form, consequentialism is "the view that normative properties depend only on consequences" (Sinnott-Armstrong, 2021). In other words, the morally right action is the one with the best overall – or *net-good*, or least harmful – consequences. It is a view which, taken literally and on its own, only takes into account future consequences of an action, assumes that harmful consequences are sufficient indicators of the moral wrongness of an action, and excludes – at least initially – the circumstances of the action, the intrinsic nature of the action or the agent, and anything that happened, was promised or agreed before the action was performed. A consequentialist evaluation of data privacy dilemmas weighs up the harms that may come from its protection or rejection against the potential benefits. The test is essentially a *cost-benefit* analysis. An overview of the literature reveals that most consequentialist theories support or reject privacy on the basis of three categories of harms, either singly or in conjunction: psychological harm, sociological harm, and/or proprietary harm. In this section, I briefly summarise each of the three categories of harms, before turning to the problems with harm-based arguments in the following section.

2.2.2. Psychological harm

The Greek Stoics (400 BCE) may have been the first to invoke a private sphere as a necessary protection against the challenges and mental distress caused by other people in the public sphere. Failing to protect the private sphere harms the emotional resilience and *ataraxia* that we need to manage the challenges of external events, public opinions and social interactions. In order to prevent the psychological harm caused by the interference of others, we need to turn our mind into a *citadel* and insulate ourselves mentally from the corrupting influence of the masses (DeBrabander, 2020:78-82). Two millennia later, in an essay generally regarded to have kickstarted the contemporary debate on privacy, a similar principle of "inviolate personality" that includes a "general right of the individual to be let alone" was introduced to justify the protection against "mental pain and distress, far greater than could be inflicted by mere bodily injury" (Warren and Brandeis, 1890:205 and 196). Positing that a right to privacy

is distinct from libel and slander, because the latter only cover material damages, the authors argue that a separate, distinct right to privacy deserves protection as a right "damnum absque injuria" (ibid:78)[18] – a right that protects against the damage or loss as a result from "mere injury to the feelings" (ibid:78) without the need to prove the actual injury. In other words, the prediction of potential psychological harm that may result from a privacy violation – such as mental distress, or "attacks upon his honour and reputation"[19] – is sufficient justification for its protection.

While most consequentialist arguments invoke psychological harm as a justification for the protection of privacy, some invoke it to justify the rejection of privacy. Richard Wasserstrom, for example, argues that privacy does nothing more than causing harmful "anxiety" that makes us "excessively vulnerable" (Wasserstrom, 1978, in Schoeman, 1984:330). Privacy is not inherently essential to the actions we tend to conduct in private. Sexual intercourse, for instance, does not in itself require privacy – in fact, it may be just as meaningful as any activity we usually perform in public, like eating dinner at a restaurant (ibid:331). The only reason why we feel a need to restrict some thoughts and activities to the private sphere, is because our social upbringing has instilled in us embarrassment and shame by means of social norms, and an anxiety to live up to these norms. The fear of being exposed, and of the resulting disapproval, contempt, and embarrassment, makes us excessively and unnecessarily vulnerable. But we should ask ourselves whether these social norms are in fact desirable features of our culture. The alternative view – "counterculture" (ibid:330) – exposes an important consequence of these cultural assumptions and presuppositions: we frantically protect information about ourselves that in fact reveals nothing more than common facts we share with everyone else. Were we to recognise that everyone has similar fantasies, desires, and fears – no matter how wicked or terrible – we would see that there is nothing to be ashamed of or anxious about. Moreover, society as a whole would be much better off with people that happily share every thought and action publicly, for two reasons (ibid:331). First, knowing that we cannot be harmed by the involuntary exposure of our actions and thoughts would make us more secure and at ease. Secondly, the absence of hypocrisy and deceit that

[18] a principle of tort law in which a person causes damage to another, but does not actually injure them

[19] Article 12 Universal Declaration of Human Rights, 1948

comes with concealing information about ourselves, would improve the quality of our interpersonal relationships – we may be able to learn a thing or two about one another and about ourselves, which we may apply for the good of society as a whole.

2.2.3. Sociological harm

Some consequentialist privacy theorists argue for the protection of privacy on the basis that failing to do so harms our societies and the proper functioning of our social institutions. Privacy is functionally required for the effective operation of a society (Merton, 1968:399), because the public, democratic debate depends on the protection of a private sphere in which opinions can freely take shape and be exchanged (Habermas 1998:417). Not protecting privacy causes social harms – it obstructs the autonomous development of ideas, free speech, free association, and other rights that are essential for the proper functioning of democracies (Magi, 2011:205).

But the impact of privacy on society has equally been invoked to argue against its protection, with arguments ranging from the common good to fairness and transparency. The first argument relies on the communitarian view that human identities are predominantly shaped by social relations and communities (Bell, 2020). From this view it is claimed that a cost-benefit analysis easily demonstrates that we protect individual privacy to the detriment of common goods, such as public safety and public health. The need to protect and contribute to these common goods requires members of communities to "move beyond self-interest" and set aside personal privacy claims (Rubinstein, 1999:228). A second argument points out the power imbalance between people, groups of people and institutions (Magi:2011:203). In the context of an Information Society this balance has been coined the *big data divide* – "the asymmetric relationship between those who collect, store, and mine large quantities of data, and those whom data collection targets" (Andrejevic, 2014). Privacy, so the argument goes, has historically been used to cover up privileges of the powerful, and as a tool of oppression (Brin, 1998). If we accept that the advancement of data technology cannot be stopped, then the only question is *who* should be given access to the data. Brin argues that the best possible answer is *everyone*, claiming that a society as a whole is better off when based on "reciprocal transparency" and "mutual accountability" rather than on secrecy. A third argument relies on

the immoral conduct privacy enables. Privacy is all too often invoked as an excuse – a societal license – for hiding immoral conduct, including conduct that perpetuates social inequalities, unequal opportunities, and abuse (Allen, 2000:1177; Etzioni, 1999; MacKinnon, 1989:116, 191).

2.2.4. Proprietary harm

The third kind of harm invoked by consequentialist arguments for and against data privacy is propriety harm. The pro-privacy argument holds that personal data has an economic value, and failing to protect that data may result in economic harm in respect of the people it relates to, or the companies and governments that have an obligation to safeguard it. Its value becomes apparent when companies are willing to supply goods and services in exchange for access to personal data (e.g. Google and Facebook), or when companies suffer economic and reputational damage from a data breach, when people monetise private aspects of their lives, or when people's personal data is exploited by criminals.[20]

However, there are consequentialist arguments for rejecting data privacy on the basis of economic harm, too. Privacy withholds important information from some, and gives unfair economic advantages to others (Posner, 1978:333). Personal data is a valuable economic good, precisely because people are willing to incur costs to be able to manage access to that information. The value of privacy is, therefore, purely instrumental. Privacy isn't valued in itself, but only as an instrument to manage something else that is valuable – information about other people. According to Posner, few people want to be *let alone* – they want to manipulate the world around them by selective disclosure of information about themselves (ibid:338). This information is valuable because it allows the person that has access to it to form an accurate picture of the person it relates to – a crucial advantage in any competitive dealings with other people. But the instrumental value of privacy doesn't stop at accessing information of competitors. People also use *false* information about themselves to try and manipulate other people's opinion of them (ibid:337). They misrepresent themselves to others with the

[20] 47% of Americans have been the victim of (financial) identity theft in 2020, amounting to US$712.4 billion (an increase of 42% from 2019). It was expected that this amount would increase again in 2021 to US$721.3 billion (giact.com/identity/us-identity-theft-the-stark-reality-report/)

aim of economically exploiting them. Defenders of privacy often invoke the right of a person to protect private information, but ignore people's and societies' right to have access to accurate information about a person we have dealings with – to *unmask* any misrepresentations – no matter how discrediting that information may be.

Seeing that the same types of harm are invoked in defence of opposing arguments may be a first indication of the unreliability of harm for our moral evaluations of data privacy. In addition, we are faced with the problem of weighing harm: which consequence is *more harmful*? Is it the social and economic harm to individuals, or to societies? Is it the mental distress of living a public life, or is it the anxiety of protecting aspects about ourselves that we in fact share with everyone else? These are questions that cannot be resolved from a purely consequential perspective. But there are more fundamental problems with a harm-based approach to data privacy, too, which we will discuss in the sections that follow.

2.3. Problems with harm-based arguments

A consequentialist approach to data privacy relies on harmful consequences – personal, social and/or economic – to justify or reject its protection. This approach assumes that we know what harm is and how we may predict it. But this assumption is also the weakness of the consequentialist approach. A brief summary of recent data privacy violations helps to illustrate the problem. Since 1984, when over 90 million Americans had their credit histories exposed in what is known as the first major personal data breach,[21] a staggering number of data breaches have been reported all over the world, affecting personal and sensitive information of billions of people.[22] In 2013, Edward Snowden caused a worldwide public uproar when he exposed highly classified, privacy-intrusive surveillance and espionage programmes run by the American National Security Agency and the Five Eyes Intelligence Alliance[23] with the cooperation of telecommunication companies and European governments. In 2018, Cambridge Analytica was publicly exposed[24] for having been given access to

[21] law.com/legaltechnews/2020/12/08/nervous-system-the-first-major-data-breach-1984/

[22] en.wikipedia.org/wiki/List_of_data_breaches

[23] an espionage alliance made up of Australia, Canada, New Zealand, the United Kingdom, and the USA

[24] wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/

personal data of 270.000 Facebook users who consented to take part in a Facebook app, but in doing so unknowingly enabled access to the raw personal data of another 87 million users who never consented and were never informed. The company "used data improperly obtained from Facebook to build voter profiles."[25] In 2019, Google, alongside various websites providing medical information and a company that manages 2600 hospitals in the USA, were investigated for exchanging medical data of website users and patients.[26] In 2021 Amazon was fined an unprecedented € 746 million by Luxembourg's National Data Protection Commission[27] for violating Europe's data privacy regulations. Amazon, like most big tech companies hardly deterred by sanctions, continues to offer the data it collects from its vast network of users and products – including shopping, IT management, reading, and household applications – to a wide range of clients via its Amazon Forecast service.[28] Closer to home, the newly established South African Information Regulator expressed its "shock at the continued compromise" of personal data of "24 million South Africans and 793,749 business entities" that had been shared with a suspected fraudster in 2020.[29]

While these headlines are an indication of the moral "outrage" and "affront" (Bloustein, 1964:156-202) most of these events have generated in the public domain, it is not always immediately clear how they have caused harm or even the potential for harm – to individuals' psychology or property, to societies and social institutions, or otherwise. To analyse whether or not they have caused harm, or have the potential to cause harm, we must say something about how we *define* and *predict* harm.

2.3.1. The problem of defining harm

While two people may agree that consequentialism is the best way to resolve moral dilemmas, they may still disagree on *exactly which* consequences ought to be given moral priority. That's because before we can weigh up good and bad consequences (and everything in between) we

[25] nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

[26] bbc.com/news/technology-50404678

[27] wired.co.uk/article/amazon-gdpr-fine

[28] docs.aws.amazon.com/forecast/latest/dg/what-is-forecast.html

[29] justice.gov.za/inforeg/docs/ms/ms-20211027-Experian.pdf

need a "sufficiently determinate, discriminating, and workable conception" (Stanton-Ife, 2022) of what good and bad is. In what follows I will argue that conceptions of harm that have so far been proposed fail to answer that question comprehensively.

Before we attempt to say what harm is, it is helpful to say what it isn't. Harm must be distinguished from the violation of a value, a virtue, or an agreement. Non-consequentialist views – such as deontological, virtue ethics, and social contract theories of morality – deem violations of this kind morally wrong in themselves, regardless of the consequences: the moral obligation is to uphold a value, virtue or agreement, not to prevent harm. Consequentialism, on the other hand, ignores values, virtues or agreements that may need to be violated in order to generate overall good, or to avoid overall harmful consequences. But this inevitably raises another question: when is a consequence *harmful*?

A number of definitions of harm have been proposed and criticised in the course of the development of consequentialism as a theory of ethics. Utilitarian concepts, for example, that define harm in simplistic terms of *pain* and *pleasure*, have turned out to be particularly problematic. Firstly, these accounts of harm are unable to explain people's willingness to endure pain (or abstain from pleasure) in exchange for values they choose to uphold. Another utilitarian attempt – the view that we must somehow distill a net good from "the greatest happiness of the greatest number" (Bentham, 1776) – swiftly turns out to be unfair to individuals or minorities, and has been criticised for enabling the "tyranny of the majority" (Mill, 1859) and "susceptible to many different definitions and pregnant with danger as a principle of policy", or even "superficial and ephemeral bourgeois ideology" (Constant, 1810 and Marx, 1867, in Crimmins, 2021). Attempts to reply to the criticisms, like Mill's distinction between "higher and lower qualities of pleasures according to the preferences of people who have experienced both kinds" (Mill 1861) do little more than further confounding the concept of harm (Brink, 2022). Other attempts have equated pleasure with the satisfaction of personal desires, and pain with its frustration (Sinnott-Armstrong, 2021:Ch3), and have defined harm as conduct that affects other people negatively, conduct that affects the interests of other people negatively, and conduct that affects the autonomy of other people (Stanton-Ife, 2022). All of these definitions, however, have provoked much criticism. The first relies on

two (false) assumptions: that people can ever act in a way that does not affect other people (most actions *do* affect other people), and that no actions can be deemed immoral if they do not harm other people. The second and third try to define one blurred concept (harm) by means of other blurred and controversial concepts (personal interests and autonomy).

Further analysis of harm has added insightful distinctions as well as further complications. *Intrinsically* harmful events, for example, are "bad for the person undergoing it" (e.g. physical pain and disease) while *extrinsic* harm is harmful "in virtue of what it brings about, not because of what it is in itself" (Bradley, 2012:392). A *comparative* account of harm defines harm as an event that makes things go worse for someone, while a *non-comparative* account requires particular 'sufficient conditions' to be present in a state of affairs for it to be harmful. For example, pain, mental or physical discomfort, disease, deformity, disability, and death, as well as having strong moral reasons against an action, constitutes sufficient conditions for harm, regardless of the benefits the harm may produce for a harmed person (Harman, 2009:139). In other words, the first defines harm as "being left in a worse state", the second as "being left in an intrinsically bad state" (de Villiers-Botha, 2020:23). A *temporal* comparative account of harm defines harm as a state of affairs in which a person is worse off compared to a state that precedes (in time) the resultant state. A *counterfactual* comparative account defines harm as a state of affairs in which a person is worse off compared to an imagined state they would be in had the harmful event not occurred. *Pro tanto* harm is harmful to some extent, but not enough to outweigh the benefits, while *all-things-considered* harm does outweigh any benefits.

In as far as non-comparative accounts rely on notions of *negative* (or *harmed*) *well-being*, they often turn out to be an empty box, because the notion of 'well-being' is so hard to pin down. For some it may mean the absence of pain or discomfort, for others, or in different circumstances, it may mean actual pleasure, or the accomplishment of projects and desires. Because there isn't agreement on what well-being means, it is impossible to agree on what harmed well-being means. It turns out, therefore, that one still has very little grasp of the nature of harm. We may try to circumvent the controversy by avoiding substantive claims about harm or well-being and define harm in a comparative way: to be harmed is simply to be

worse off. A person is harmed if it can be shown that they are worse off than they would be in a (temporal or counterfactual) comparatively alternative state. But here again there are problems: we can think of examples where people have been clearly harmed but are not relatively worse off (e.g. stealing from a billionaire, or donating a kidney), or where people are clearly worse off without being harmed (e.g. when sensitive or embarrassing information about them is published). In respect of the latter, Warren and Brandeis' above-mentioned definition of the right to privacy as a *damnum absque injuria* comes to mind: privacy is a right that protects against being worse off (injury to the feelings) without the need to prove the actual harm (Warren and Brandeis, 1890, in Schoeman:78).

The difficulties with harm conceptions and the open-ended debates they have provoked have led some authors to point out an apparent contradiction between the fact that, on the one hand we find social injunctions against harm everywhere, but on the other hand "nobody bothers to say what it is" and when they do, we find a "mess" (Bradley, 2012:391). Others have echoed this frustration, by writing that "the meaning of 'harm' is generally left up to our intuitions, potentially further exacerbating ethical disputes" (de Villiers-Botha, 2020:21). Even those that argue on the basis of Mill's harm principle (Mill, 1859:265) conduct their arguments without defining what they mean with the concept of harm (Stanton-Ife, 2022). It is a frustration, if based in truth, that is well justified: we ought to question the validity of an ethical theory that relies on presumed conceptions of harm that are themselves fundamentally flawed.

Perhaps it is a frustration that gives us enough reason to stop trying to define harm altogether, and replace this "Frankensteinian jumble" with "more well-behaved concepts" (Bradley, 2012:391). Neither comparative nor non-comparative accounts of harm hold up against a list of *desiderata* any account of harm ought to be able to account for. That is, it must not rely on presumptions of well-being or morality ("axiological neutrality", ibid:394), and must be able to explain what *all* harms in all degrees have in common, and why we ought to try to avoid and prohibit them by means of normative, deontological restrictions. From this, Bradley concludes that all known accounts of harm "should be jettisoned for purposes of philosophical theorising" (ibid:396). We are looking for explanations of harm in the wrong place. "Our judgments about harm are muddied by moralising. (…) We are more likely to call an act

harmful if we think it is wrong. Perhaps (…) impermissibility has to do with rights, justice, or desert" (ibid:410). Perhaps, what Bradley means is that we ought to define harm in terms of *values*.

Others argue that we should not give up that easily. Dissatisfaction with current definitions of harm does not necessarily mean that adequately defining harm is impossible or undesirable. To say so is "premature and impracticable" – it's hard to see how we could proceed with moral theorising without some concept of harm (de Villiers-Botha, 2020:22). Focusing her analysis of harm on the question of what it means to *be* harmed rather than on the question of what it means to *cause* harm, de Villiers-Botha points out problems with comparative accounts of harm that avoid substantive claims of harm, and concludes that it is "unclear how far this apparent axiological neutrality can take us" (ibid:24-26). After all, claiming that someone is *worse off* presumes that we have an idea of what it *means* to be worse off. This is simply impossible without some kind of reference to a substantive, non-comparative theory of well-being (ibid:24). But on the other hand we cannot rely on non-comparative accounts either, because these accounts are problematic for their own reasons – most notably their failure to explain what unifies all harm. The way out of this stalemate, de Villiers-Botha suggests, is by "changing the perspective from which harms are attributed." After all, what does in fact unify all accounts of harm, is what harm means *for those affected by it*. Harm is not defined in a universal list of intrinsic conditions, but defined as *bad* in a "subject-relative sense" (ibid:27). In other words, harm can only be defined from the perspective of an affected person, and is only bad in as far as this person evaluates it to be bad. This means that people get to decide for themselves, from their own perspective, how harm compares to benefits (or other concerns and interests), and whether or not to *consent* (ibid:28) to what others, from their perspective, may view as harmful (e.g. death may be seen as a great harm, but may be valued differently by a person suffering from an agonising illness). So, whether or not harm is considered *bad* depends on the subjective perspective of those affected by it – that is, on how they *value* a particular state of affairs. But before a being can value any state of affairs it needs to be of a "value-fixing-kind" (ibid:28). That is, it needs to be able to value a particular state of affairs against a sense of its own "welfare – it must be possible for things to go better or worse for it" (ibid:28). This is not a rational consideration, but a matter of (a very broad

conception of) "preferences and aversions" which may include "all of the things that we value or might value without necessarily (currently or ever) being aware [of their being preferences or aversions]" (ibid:29). Every *value-fixing* being avoids a state of affairs that goes against their own welfare – that holds "negative prudential value." To be harmed then means "to be subjected to something that holds negative prudential value for one (…) for a variety of reasons, both intrinsic and extrinsic" (ibid:29).

However, Bradley's appeal to rights, justice and desert, and de Villiers-Botha's reliance on personal valuations, fail to resolve a recurring problem with all accounts of harm: the *perspective* from which harm is defined. Either harm is the same for everyone, and we prevent it by means of universal norms, or harm is subjective, and each and everyone must decide and negotiate for themselves when protection is required. If it is a general concept, then we may predict it with some accuracy as a society, prevent and regulate it in terms that equally apply to all members of society, and bear the risks and responsibility for getting our predictions wrong as a society. A subjective account of harm, on the other hand, demands each and everyone of us to evaluate and negotiate with others what harm is, make predictions, accept the risks and bear the responsibilities when predictions turn out to be wrong. But there are fundamental problems with subjective accounts of harm. De Villiers-Botha's claim that we would be able to unify all harms when we shift our focus to subjective conceptions of harm (ibid:28) seems misleading, if all it does is to claim that harm is whatever someone subjectively values as such. She may reply that this is the only perspective that counts, really, because all that matters is how harm is valued by those affected by it (ibid:30). But it leaves other questions open. In the absence of a unifying, common denominator that accounts for *all* subjective accounts of harm, how do we regulate and prevent harm as a society – assuming that society has a moral obligation to inform and protect people against harms they cannot possibly know or are unable to mitigate? Perhaps what de Villiers-Botha implies, is that we can't. We must resort to norms that are agreed between particular people in particular circumstances, by means of consent (ibid:28). But even if we leave it up to individuals to decide and negotiate for themselves what harm is and how much of it they are willing to endure, how do we as a society weigh up different harms for different people, and decide which carries the heaviest moral weight in a consequential cost-benefit analysis? If, for

example, the subjective badness of a privacy violation is valued differently by every person, how will we ever agree on how we manage data privacy? Without a common denominator, how do we morally weigh up subjective harms? Moreover, subjective accounts of harm make it impossible to *predict* harm at the individual level. Remember that we have set out to define harm for the purpose of being able to compare different harmful consequences in order to decide which consequence ought to be given moral priority. But if we reduce harm to mere subjective experiences and valuations, how do we predict how this or that person will value a particular consequence? This brings us to our second challenge to a harm-based approach of data privacy: predictability.

2.3.2. The problem of predicting harm

We have so far attempted to define what it means to *be* harmed. But, assuming that we could ever agree on a definition of harm, a moral obligation to protect people from harm implies that we understand what causes it, and how we may prevent it. But in order to prevent, we must be able to predict. This raises questions of knowledge, culpable ignorance and risk. How can we possibly know all consequences of an action? Are we responsible for all consequences – even those we are not aware of? And to what extent should we be allowed to take the risk of not knowing?

We may reply to the first question that we can't – we simply cannot know all possible consequences of an action. Which is why we must only focus on consequences that we are capable of knowing. This view, known as *proximate cause,* underpins legal interpretations of consequentialism. It defines the legality of an action by analysing the direct causal chain between an action and proximate (that is, known) consequences that are directly caused by the action. For morality, this would mean that the moral rightness of an action no longer requires us to predict and take into account all possible non-proximate consequences (Sinnott-Armstrong, 2021). However, some claim that to raise this question is a misrepresentation of consequentialism. Doing so presumes that consequentialism should be able to provide some sort of magic formula for whipping up practical answers to our moral dilemmas. But consequentialism is not a decision procedure, so the argument goes. Rather than providing clearcut answers, it sets out criteria – that is, necessary and sufficient conditions – *at a higher*

level for actions to be morally right. Whether or not an agent can tell in advance whether those conditions are in fact met, is irrelevant for the moral evaluation of her actions (Sinnott-Armstrong, 2021). To put this differently, consequentialism shapes a moral landscape, it does not tell us what to do. In fact, most contemporary consequentialists admit that consequences may sometimes point us in the wrong direction if we take them too literally and in isolation from other concerns. Consequentialism may not always be the best possible procedure to maximise benefits (utility), because it may produce unfair results when it is exploited by "an elite group that is better at calculating utilities" (Sidgwick 1907, 489–90, in Sinnott-Armstrong, 2021), and most moral agents may be better off when following their moral intuitions, "because these intuitions evolved to lead us to perform acts that maximise utility, at least in likely circumstances" (Hare 1981:46,47, in Sinnott-Armstrong, 2021).

However, separating higher-order moral criteria from practical moral considerations is no simple matter. Isn't the rightness of a particular moral action always derived from higher-order moral criteria? One may argue that this is not necessarily so – higher-order criteria may differ from lower-level considerations, for example in the context of stock investments. Whereas the higher-order criterion of investment is obviously maximising profit, lower-level decisions may be motivated by other criteria, such as risk-reduction – in ways that are consistent with one another (Derek Parfit, 1984, in Sinnott-Armstrong, 2021). However, is the consideration to reduce risk not directly derived from a profit-maximising criterion? If the higher-level criterion were maximising loss, then surely risk-reduction would not be a consideration. It does not make sense to separate one from the other. We can even think of examples that positively confirm that lower-level and higher-level criteria cannot be separated. Take, for argument's sake, a rugby game. On the one hand, higher-level criteria are set by the overall strategy the team agrees on (offensive, defensive, and whatnot). But it would not make sense to claim that, once on the field, each and every action of the players is not directly determined by the higher-order strategy. In fact, for this higher-order strategy to make sense at all, each and every player must act in ways that are consistent with that strategy. Returning to consequentialism, it does not make sense to claim that all consequences of an action set out the criteria of morality at a higher level on the one hand, but some

consequences may be ignored in our practical moral considerations because we aren't capable of knowing them, on the other hand.

When it comes to our second question of whether we should be held responsible for harm we did not predict or could not even be aware of, most authors seem to agree on two arguments, but disagree on where to draw the line. On the one hand, the moral obligation to prevent harm operates on a "*defeasible* presumption of responsibility" (Rosen, 2003:61, my italics) – that is, the presumed responsibility for harm we apply to people in general may be excused under certain conditions. On the other hand, where possible, moral agents have a duty to "rectify their culpable ignorance in order to avoid acting upon it" (Vanderheiden, 2016). A number of concepts have been suggested to test culpability for harm. Gideon Rosen, for example, argues that three "epistemic irresponsibilities" drive our culpability for ignorance: people are to be blamed for the harm their actions cause if they are *reckless*, *negligent* or *deliberately* lacking in the obligation to inform themselves, adding that this obligation "varies massively from case to case" (Rosen, 2003:63). Holly Smith suggest that we ought not to excuse people for the harm they cause when one of three scenarios applies: when people fail to do their homework, when people have set themselves up in a way that prevented them from being aware of the wrongness of the action (e.g. they got drunk before getting into a car and killing a pedestrian), and given what they already know, people fail to make inferences that may generally be expected of them, as persons with normal cognitive capacities (Smith, 1983:544). Steve Vanderheiden adds that a number of factors need to be weighed in our judgements of culpable ignorance, including the availability of information, the cost of acquiring information, the agent's cognitive capacity to process and deliberate available information, collective versus individual responsibility (with a greater responsibility for collectives), the context (the higher the moral values and consequential harm that are at stake, the greater the duty to rectify ignorance), the range of moral challenges (in time and space, here and now versus far away and in the distant past or future), the distance (in time and space) of the harm that results from ignorance, reasonability (what would a reasonable person have known, or should have known, or have done to acquire knowledge?), and the ignorance of our ignorance. He concludes that people can only be held responsible for not making "sufficient efforts to obtain" knowledge of moral or empirical facts that would have enabled them to prevent harm. We cannot blame

them for remaining ignorant about [these facts] (Vanderheiden, 2016:305). Here again we find an argument against a harm-based approach of data privacy: how do we determine whether people have been recklessly or deliberately neglecting their obligation to inform themselves, when it is claimed that data privacy rights have been violated?

Lastly, in reply to our third question as to what extent we should be allowed to take the risk of not knowing, we must say something about the ethics of risk. Moral responsibility for the consequences of our actions is not only a function of our obligation to know what these consequences may be, but also of the risks we condone when we remain ignorant of these consequences. Whether or not this ignorance is excusable, we take a risk if we act in the absence of knowledge of the full range of consequences. We may say that the less we know, the more risk we take. We may say that the less we know, the more risk we take. But how much risk is ethically justifiable? A risk constitutes a *possibility* of harm, and in this sense a principle of respect for persons implies that everybody has a right not to be exposed to risk by others. But risk is not actual harm, so we cannot apply the same protections as we do for actual harm. Doing so would make life simply impossible: everybody acts every second of the day in ways that may potentially endanger other people, e.g. by driving a car, holding a baby or forwarding a malicious email. It is for this reason that Sven Ove Hansson argues that our right not to be exposed to risk by others is a *defeasible right* – that is, exposure to risk is acceptable only if the exposure is part of an established, "justice-seeking" social practice, and the affected people have a say in it, and are willing to accept the exposure in exchange for "advantages" (Hansson, 2013). It is crucial for any risk analysis to identify the roles, or combinations of roles, that play a part in the risk exposure. Hansson suggests that we steer clear from risks that clearly stand to benefit one party while harming another. Morally defensible risks would be cases that centralise benefits, harms and decisional power into one party (*individualism*) or equally distribute benefits, harms and decisional power among all parties (*adjudication*) (Hansson, 2018). Hansson's *Ethical Risk Analysis* is particularly useful for the argument in this thesis, because it analyses risk in terms of who bears the (potential) costs, who reaps the (potential) benefits, and who decides whether or not the risk is taken or allowed to continue. I will return to these concerns when I discuss the concept of 'informed consent'. But again, we may ask whether it is justified to rely on the prediction of harmful

consequences to decide whether or not people should be exposed to data privacy risks, when we have no way of knowing what all potential consequences may be.

2.3.3. Consequentialism in the Information Society

I have so far argued that consequentialism relies on flawed presumptions of harm and predictability. From this I conclude that consequentialism is, on its own, bound to come up with flawed answers to our moral dilemmas. One may oppose this conclusion, and retort that I cannot make this claim in general terms, either because it is not necessarily true that a moral view that relies on flawed assumptions can only produce flawed answers, or because conceptions of harm and predictability are in fact not as flawed as I have presented them above. Be that as it may, what cannot be denied is that a "world made increasingly more complex and unpredictable by emerging technologies" (Vallor, 2016:1) further *weakens* presumptions of harm and predictability, and *strengthens* the argument against moral reasoning that relies on these presumptions.

The 'new world' I have introduced in Chapter One makes consequentialist predictions about the future nearly impossible. Replying to the critique that predicting utilitarian outcomes requires time – time that we generally don't have when faced with moral dilemmas – Mill points out that our notions of good and bad are concepts that have developed over "ample time, namely, the whole past duration of the human species" (Mill, 1863 in Shafer-Landau, 2013:420). In other words, consequentialists do not have to re-invent mankind's most basic moral codes every time they conduct a cost-benefit analysis – even consequentialists rely on established principles of morality that have come down to us via previous generations. But for humankind to rely on socially and historically developed notions of morality, we must be able to assume that our living conditions have not fundamentally changed, and that our contemporaries as well as future generations face essentially similar moral challenges. Whereas ethicists in the past could rely on this assumption, this is no longer the case today. Today's ethics is characterised by *acute technosocial opacity* – "rapid technological, sociopolitical, and environmental change accompanied by existential risks that make the ethical pursuit of the good life in the 21st century extraordinarily challenging and fraught with uncertainty" (Vallor, 2016:23). Not only is it nearly impossible to predict new technologies,

more importantly is the impossibility to predict the social, economic and political impact of new technologies, which is evidenced in all the unpredicted ways we manage today's technologies (ibid:8).

Of course, a world that is difficult to predict or understand is not necessarily a harmful world. A consequentialist approach would require us to weigh up all the harms against all the benefits – potential as well as actual, demonstrable benefits. This leads some authors to argue that the benefits of data privacy violations clearly *outweigh* the potential costs. First, there are good reasons to accept some harms in exchange for the abundance of social, economic and political goods that we are getting in return. The trade in personal data has produced a plethora of useful applications for our individual and social health and wealth. The commercial value of personal data keeps many essential digital services free and equally accessible to everyone. As a matter of fact, the revenues big tech companies generate in one (rich) part of the world allows them to make their services freely available to other (poor) parts of the world. This is effectively a value transfer from the global rich to the global poor (Gilbert, 2021:59). It creates unprecedented opportunities too, from "being able to communicate with friends and family, grow businesses, build networks and so on" to "wide distribution of power that can be mobilised by anyone" (Gilbert, 2020:162 and 166). Social institutions and groups, particularly marginalised groups, benefit enormously from the exchange of personal data. Movements like #metoo and #blacklivesmatter would have been impossible without the public exchange of intimate, deeply personal stories about sexual exploitation and racial discrimination. Established social institutions which are traditionally hampered by unequal access, like the free market and democracy, benefit from the unhindered exchange of personal data too. Economic agents are connected to one another in unprecedented ways that contribute to fair access to the market – socially, geographically, and financially. Citizens of democracies have unprecedented platforms to express and deliberate opinions in ways that contribute to fair access to the democratic process.

Secondly, there is in itself nothing necessarily harmful about the fact that a lot of personal data about a lot of people is in the hands of a few. The business models of big tech companies are not built on wielding power over (let alone, harming) individual people, but on learning,

predicting, and commercialising trends in human thinking and behaviour. Tech companies do not trade in specific people's personal data – that is not where the value of that data lies. In fact, they encourage people to control how their personal data is being used – by means of transparent, user-friendly privacy tools and the ability to opt-out of certain kinds of data processing. With these controls in place, how much personal data people end up sharing is ultimately a matter of personal preference, not of ethics (Gilbert, 2021:15). This is demonstrated, for example, most recently by Google's announcement to do away with cookies that track individual online behaviour in favour of so-called *FLoCs* or *Topics* that track cohorts of people that display similar online activity and preferences. Moreover, even *if* tech companies or governments wanted to manipulate each and everyone of us, they couldn't: their actions are largely based on behavioural data (as opposed to profile data) that is aggregated partly from individual but mostly from mass behavioural patterns, and that allows them to make nothing more than *educated guesses* – they do not zoom in or exploit personal character traits. Tech companies and data brokers take something that is useless in itself and turn it into something valuable. There is nothing wrong with that, and this does not infringe upon anybody's moral or property claims. Nobody puts this better than Sam Gilbert: "Rather than oil, a better metaphor for data might be manure. Like most data, manure is a mundane by-product of life, and there are businesses that have built the logistics to collect it on a large scale and process it into something useful: fertiliser for their crops" (Gilbert, 2021:21, 22, 28).

However, these consequentialist arguments in favour of technological progress to the detriment of data privacy suffer from a number of flaws. To begin with, they apply a moral concept of privacy developed in an earlier era to our new privacy concerns. We have already discussed Floridi's argument against the 2P2Q hypothesis, and the unprecedented challenges new technologies pose to data privacy. We may point out fundamental problems with the Theory of Technological Determinism, too (Chandler, 1995), and argue that we are in control of how technology shapes us – not the other way round. The theory is reductionistic – it incorrectly presents history as a progression of technologies, and denies the many other factors that determine human behaviour and development. It is also mechanistic – it claims that technology causes changes in the behaviour of all who use the technologies in casually predictable ways, and it is reifying – it elevates technological abstractions and inanimate

objects (e.g. the internet, social media, or smartphones) to the level of entities with intentions, desires and needs of their own. The Theory of Technological Determinism presumes technological autonomy, or the belief that technology is self-generating, rather than designed, used, valued and managed by people, and therefore necessitates an autonomous, inevitable self-evolution of that technology. Lastly, it presumes a technological imperative, or the belief that technology must be used simply because we have been able to design it – once it is there, we cannot not use it.

Shoshana Zuboff takes the argument that technology does not shape itself, but we do, one step further. She gives the underlying ideology which ultimately shapes new technologies a name: *surveillance capitalism* (Zuboff, 2019). Privacy challenges of the nature and degree in which they occur today are not merely by-products of new technologies. There are *reasons* for why new technologies are designed and managed in ways that are in their very essence privacy-intrusive. These reasons are motivated by an ideology that provides a moral justification for preying on data about (private) human behaviour and using or trading that data for purposes that are ultimately nothing more than commercial: prediction, manipulation and competition. When it comes to the presumed inevitability of the Information Society's ubiquitous privacy violations, Zuboff argues that "surveillance capitalism is a logic in action and not a technology" (Zuboff, 2019). Surveillance capitalists make us believe that private violations are inevitable and harmless by-products of the technologies they employ, while in fact they are "meticulously calculated and lavishly funded means to self-dealing commercial ends" (Zuboff, 2019). In other words, the way new technologies relate to data privacy is not an inevitable result of technological progress, but the result of how surveillance capitalists choose to target people. In Zuboff's view, the moral choices tech companies make with regard to people's privacy are motivated by "instrumentarian power [that] aims to organise, herd, and tune society to achieve a (…) social confluence, in which group pressure and computational certainty replace politics and democracy, extinguishing the felt reality and social function of an individualised existence" (Zuboff, 2019:470). After all, tech companies and the economic and political interests that fund them, aspire to create models from the private data they collect that allow for the prediction of people's economic and political behaviour – and what better way to predict behaviour is there than to create and manipulate it?

A second contestation takes aim at the problems of anonymous and de-identified data, which I've introduced earlier. Anonymisation and de-identification claims can all too often not be verified or guaranteed. In fact, we often don't know how anonymous information really is. Private data is by its very nature vulnerable, and exposed to opportunities for abuse every time it is shared among data brokers and processors. A New York Times investigation[30] found that a test subject's precise but anonymous geolocation data was recorded by 75 companies 8,600 times over a period of four months – on average, once every 21 minutes. This implies that once this data has been collected it may be shared with numerous (scrupulous and less scrupulous) companies anywhere in the world, for any kinds of purposes. While these companies claim that they are interested in the patterns, not in individually identifiable information, the real question is not what is currently and knowingly done with the raw data, but what can be done, or what can be done with new technologies in the future. Anyone with access to raw location data can, in fact, easily consult public records to find out who lives at a particular location that they have tracked anonymously. This was demonstrated by one group of researchers claiming that "99.98% of Americans would be correctly re-identified in any dataset using 15 demographic attributes" (Rocher, Hendrickx and de Montjoye, 2019), after another group of researchers had claimed that "four spatio-temporal points are enough to uniquely identify 95% of the individuals" (de Montjoye, Hidalgo, Verleysen, *et al.,* 2013). We may think of other examples too – examples that do not require hitherto unknown applications of technologies, but only require a new moral landscape, like a change of government. Sensitive information that is collected by one government in support of its populations, may be used by another government against these populations – as was demonstrated by the Nazis in the Second World War (Véliz, 2020:112). A more recent example is found in Afghanistan, where citizens fear reprisals at the hands of the new Taliban government that may use existing "biometric databases and their own digital history (…) to track and target them."[31]

---

[30] Valentino-Devries J., Singer N., Keller MH and Krolik A (2018) *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret.* The New York Times. Available at nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

[31] reuters.com/article/afghanistan-tech-conflict-idUSL8N2PO1FH

This concise overview demonstrates the weakness of harm-based arguments for or against data privacy: the uncertainties, and the lack of transparency and understanding that pervade the current, unprecedented technosocial context make it impossible to claim anything beyond estimations and correlations of harm. We simply do not know the extent of the harm data privacy violations cause. A consequentialist perspective does not allow us to weigh up the harms that result from privacy violations versus the harms that result from its protection. And we simply don't know how future technologies will manage to harm us with the personal data that is currently being collected. It is not unthinkable that we will in fact rely on technology to protect our privacy in the future.

2.4. Conclusion

I have argued in this chapter that we cannot know with any degree of certainty what the consequential harms of data privacy violations are, or will turn out to be, in the current context of a rapidly changing Information Society. I have also argued that, even in the event that we would be able to predict these harms, they may be valued differently by different people in different circumstances. However, this does not mean that data privacy violations are necessarily harmless, or that their actual or estimated, causal or correlated, harms must be ignored entirely. It is undeniable that consequentialism plays a role in our moral reasoning: the consequences of our actions contribute to the criteria for moral permissibility and responsibility. But the extent of that role is inversely proportional to the complexity of the moral landscape. The concepts of harm and predictability are controversial at the best of times, but rapid and complex technological innovation crucially undermines their reliability. We have reasons to believe that the ways in which personal data about people is being processed by new ICTs are "all the more dangerous because they cannot be reduced to known harms (…) and therefore do not easily yield to known forms of combat" (Zuboff, 2019:1081). This means that we cannot rely solely on allegations of harm to make sense of our moral concerns around data privacy. However, this is not an argument to throw in the towel, to ridicule the estimations of harm, and to walk away from the debate. Rather, it is an argument to move from an inconclusive debate that is undermined by unreliable claims, to a debate that is motivated by the need to protect our most important moral values. Rather than discussing arguments that rely on what we don't know, we ought to deliberate arguments that rely on

what we do know. What we do know, is that each and every person deserves respect. We know this for a fact, because this very principle shapes the foundations of our liberal societies and our most important social and moral contracts, such as the Universal Declaration of Human Rights. Given this principle, I will argue in the next and final chapter that respecting persons implies protecting privacy.

3. ARGUMENTS FOR A VALUE-BASED APPROACH

3.1. Introduction

In this chapter, I defend a value-based approach to data privacy as an alternative to the harm-based approach discussed in the previous chapter. As I will show, the primary ethical challenge is not to try and predict the benefits or costs of data privacy, but to set out the moral criteria for evaluating data privacy challenges today and in our *technosocial* future (Vallor, 2016:5). My argument for a value-based approach to data privacy is essentially an argument for setting boundaries for and taking control of how technology develops – contra the *Theory of Technological Determinism* (Chandler, 1995) discussed in Chapter Two.

However, such a value-based approach seems to run into an immediate problem: some of our moral values may be mutually incompatible. For example, the individual right to privacy may be at loggerheads with the right to freedom of expression, freedom of the press, and the right of access to information. This reveals the core question of our data privacy concerns: how do we balance opposing values in ways that are morally defensible? In this final chapter of the thesis, I develop a justification for data privacy as an intrinsic value and suggest a procedure for deliberating about and managing conflicts between data privacy and other values. First, I discuss what values are and why they deserve our protection. Next, I introduce the principle of respect for persons, and its relationship to the concept of privacy. This will lead us to the central argument of this thesis: because the moral value of respect for persons qua persons deserves protection, and because persons cannot be persons in the absence of some degree of privacy, therefore privacy deserves protection. In reply to possible challenges to a value-based approach, I show that the criticisms I have raised in the previous chapter in respect of a consequentialist approach do not apply here: values are not predicted benefits, value trade-offs are not cost-benefit analyses or inherently contradictory, and current data privacy concerns cannot be reduced to other moral concerns. I end this chapter with a proposal for deliberating data protection concerns in relation to other moral concerns, and an example of how this deliberation would play out in the field.

3.2. Value theory

The philosophical study of values (axiology) defines values as "criteria by which we evaluate states of affairs and the choices that lead to them" (Baron, 2017:85). To put this differently, protecting or rejecting values are a way of attributing "goodness and badness to some thing, person, relationship, act, or state of affairs" (Anderson, 1993:1). Values may be intrinsic – that is, in virtue of their own, inherent properties – or extrinsic – that is, instrumental for the value of something else (Schroeder, 2021). Not only do we find ourselves *having* and *expressing* values by means of 'subscribing' to a particular value or 'ascribing' a value to other persons, events, or states of affairs (Rescher, 1969:3), but we also make normative "value judgments" or evaluations that seek to *justify* (or reject) these attitudes (Edel, 1953:198).

Values represent our vision of how we think the world ought to be and how we ought to live in it – our vision of the *good life* (Rescher, 1969:4 and 10). While this definition of value seems uncontroversial at first, the philosophical study of value is at least as widely contested as the study of harm (Edel, 1953:201). One contestation involves defining what is, or what ought to be, valued as good. Its arguments range from singular universal concepts (Anderson, 1993:15) to pluralistic, historically and socially contingent concepts (Anderson, 1993:15), and from naturalistic and objectively verifiable concepts (Perry, 1954:4,5; Dewey, 1939) to emotive expressions (Stevenson, 1944) and intuitions (Moore, 1903). Like the discussion of harm, the contestation around the source of values is essentially animated by a disagreement on whether values are subjective or universal. Everyone agrees that some values are simply a matter of personal preference, and that some things are only good from a particular point of view – that is, good for a particular person or in particular circumstances. For example, one may value a cup of coffee, without inferring any claim about how the next person ought to feel about coffee. Some people may not value coffee at all, and coffee may in fact not be that good for some people, or in certain circumstances, e.g. right before bedtime. But this is not the kind of values the study of ethics is interested in, and not the main point of disagreement. From an ethical perspective, a more important question is: are there things that can be deemed good for everyone – simpliciter, from an objective, universal point of view? If answered affirmatively, it would mean that some values have a normative quality, in the sense that everyone has a moral obligation to uphold them. If, for example, the value of coffee were

objective and universal, it would mean that everyone would have a moral obligation to value and protect coffee, regardless of personal preferences and contingencies. It is a question, however, that is preceded by another: if some values do indeed carry universal moral weight, where does that weight come from? What justifies it? To this question, some have argued that values are defined by abstract, universal concepts. Rescher, for example, defines values as "perfectly objective standards revolving about the concept of human welfare" (ibid:10). But, as we have seen earlier in our discussion of harm, definitions of human welfare are widely contested. In addition, relying on universal standards runs the risk of detaching abstract values from the practical circumstances they apply to. And the assumption of perfectly objective values doesn't account for the conflicts of values every moral agent faces from time to time. In reply, I argue for a different approach: some values derive objective moral authority, not from where they are found, but from how they *relate to other values*. A great deal of our justification of moral values rests on demonstrating that they are supported by other values. Consequently, as I will argue in the last section of this chapter, the only way to resolve value conflicts is by means of a rational deliberation of values. However, values are not perfectly objective and abstract – somehow hovering over and above the practical moral challenges we face in the world. A value-based approach therefore not only seeks rational coherence, but also seeks to balance values with the circumstances they apply to. The approach I have in mind, in other words, seeks to balance practical challenges with a coherent vision of the good life. It is in this balance that the source of values must be found.

This brings us to another contestation: the question of the relationship between values. Rescher argues that values are inextricably associated with the fact that people are rational, goal-oriented agents, and that values rationalise and justify our actions (Rescher:1969:9 and 11). I agree with this claim: if we wish to make objective, normative value claims, we need to rely on objectively – that is rationally coherent – verifiable arguments. However, the claim that all values are, can or must somehow be logically consistent does not account for value conflicts. Rescher omits an important distinction from his analysis: values relate to other values *vertically* as well as *horizontally*. By *vertical* I mean that some values logically derive from other values. Subscribing to one value requires us to subscribe to other values that are rationally compatible with it. Rescher's terminology of value object, locus of value, and

underlying value, is helpful to illustrate this vertical relationship between values. The *value object* refers to what we are evaluating. This can be anything from things, animals, people, actions, states of affairs, plans and policies, etc. (ibid:8) to, for example, the ways in which personal data is processed by ICT. The *locus of value* indicates a particular desired, valued state of affairs, for example privacy. But further analysis reveals that the locus is not the *underlying*, or "proper" value (ibid.8) that essentially motivates our evaluation – something more "remote, abstract, and ideological" is what really animates our evaluation. In the case of privacy, as I argue in the next section, this underlying value is the principle of respect for persons.

However, this vertical logical coherence between values does not make sense when we are challenged by horizontal value conflicts. By *horizontal* I mean that every value relates to other, sometimes opposing values, that in their totality make up a coherent moral framework – for example, that of liberal democracy. Subscribing to horizontally opposing values is not irrational or incoherent if these values make sense within a broader moral framework. For example, even though the right to privacy and the right of access to information protect horizontally opposing values, they are vertically consistent with the underlying value of respect for persons, and coherent with the liberal democratic ideal. As a result, when horizontally opposing values are at stake, a rational balance must be deliberated on the based of arguments that are compatible with our broader framework of morality. In other words, any suspension of a value must be based on good reasons that are themselves conducive to the overall good life we envision. The right to data privacy, for example, must at all times be balanced with other moral concerns, which can be as broad as the right to freedom of expression, freedom of the press, the right of access to information, the right to personal and collective security, the moral obligation to contribute to, or at least not obstruct, human welfare, etc. In the next sections, we will see how the above analysis of value applies to data privacy, starting with its underlying value: the principle of respect for persons.

3.3. The principle of respect for persons

From the 18th century onward, privacy became part of a larger social, economic and political project that culminated in the establishment of liberal democracies around the world, in which

respect for freedom and autonomy of every person features as a primary, foundational principle (Bloustein, 1964:165) – or in Rescher's terminology: an *underlying* value (Rescher, 1969:8). This principle is rooted in the writings of some of the most influential thinkers of that era (Courtland, Gaus, and Schmidtz, 2022). For Kant, for example, "The idea of freedom as autonomy (…) contains first and foremost the idea of laws made and laid down by oneself, and, in virtue of this, laws that have decisive authority over oneself" (Johnson and Cureton, 2022). Kant defines the principle of respect for persons as the moral and unconditional requirement to always acknowledge, value and protect the dignity of every person, simply because they are persons, or "ends in themselves" and not merely means to an end (Dillon, 2020). John Stuart Mill, another important proponent of the liberal ideal, argues that everyone has a moral right to develop their individuality to the best they can be, as well as a right to protection against anything that interferes with this development (Habibi, 1996:90).

The value of privacy is essentially connected to the principle of respect for persons and its associated freedoms (Benn, 1971: 231 and 239). The spread of liberal democracy around the world may explain why privacy only became a serious matter of philosophical (and legal) contemplation from the 18th century onward. The liberal justification for privacy can be summarised as follows: if we accept that each and every person deserves respect and protection simply because they are a person, and we accept that people need privacy to be persons, then it follows that we must protect privacy. We find this connection between privacy and the principle of respect for persons in a great deal of ethical theories of privacy. Thus we read that fundamental human values of "individual dignity and integrity" and "individual freedom and independence" are the common denominators that unify our moral concerns for privacy (Bloustein, 1964:163). Or that privacy protects persons qua persons – persons as ends in themselves (not means to an end) – and its violations therefore "injure [people] in their very humanity" (Fried, 1968:203 and 206). Others argue, in a similar vein, that a person is "a source of value" (Schoeman, 1984:414), a "subject with a consciousness of himself as agent, one who is capable of having projects, and assessing his achievements in relation to them" (Benn, 1971:228). What all these theories argue, is that a person simply stops being a person when all of their ideas, actions, projects, relationships, and preferences are controlled by

external interference, and the principle of respect for persons simply evaporates when these essential aspects of personhood are denied or merge with the mass (Bloustein, 1964:188).

3.4. Privacy is a value

I now intend to develop my argument for why privacy is an intrinsic, objective value that deserves protection, in two steps. The first step is a conceptual analysis of the unique conditions, or intrinsic characteristics, of privacy: what is private, and what constitutes a private sphere? A clear understanding of the concept of privacy will enable us to move on to the next step: a moral evaluation of why privacy deserves protection.

3.4.1. The intrinsic characteristics of the private sphere and its violations

We have already considered – and rejected – the argument that privacy is instrumentally valuable as a means of preventing harm. However, privacy features as an instrumental value in other arguments as well. In all these cases, privacy is treated as a necessary means for the protection of something that has nothing to do with privacy. Aristotle, for example, treats privacy as a necessary condition for people to make up their own minds, by turning away from the public sphere in order to "transform common opinion into right opinion" and "achieve excellence" in the private virtues associated with family, friends, business, and philosophical contemplation (Swanson, 1992:1-8). However, his ultimate justification for privacy has little to do with the protection of persons. Rather, privacy allows people to become better at public affairs: the public sphere benefits from the virtues people develop in private, because people "carry virtue earned in private into the public" (ibid:3). Many contemporary arguments share Aristotle's assumption that the protection of privacy is a social good in so far as it contributes to a better society (Kasper, 2007:185; Merton, 1968:399; Habermas 1998:417;Magi, 2011:205).

However, if privacy were a purely instrumental value, it would be dispensable if it can be shown that its objectives may be accomplished by other means. For example, if the need to protect sensitive personal data were only motivated by the need to prevent this data from falling into the wrong hands and the harms this may cause, then measures and tools can be put in place to strictly control and secure who has access to personal data without any reference to

the concept of privacy (Fried, 1968:203). Or if privacy were only instrumental in protecting personal liberty, that too, can be accomplished by other means (ibid:210). However, even when security measures and guarantees for our personal freedom are in place, we still feel a need for privacy. Data protection does not cover all our privacy concerns. This, according to Fried, shows that privacy is much more than a mere social instrument to protect other interests (ibid:205). An instrumental conception of privacy does not fully explain our privacy concerns. It overlooks the deeper moral concern that underlies our valuation of privacy. To understand the more fundamental moral concern that lies behind our privacy concerns, I will first look at what characterises a private sphere, and secondly argue why a private sphere deserves protection.

The private sphere can be defined as a zone that is "immune from specified interventions" and protected by social norms of varying explicitness and force (Scanlon, 1975:316-319); or as areas of human life that inherently deserve protection against interference (Benn, 1971:236). These are merely formal definitions. Other authors, however, argue more substantive accounts of what defines privacy: privacy is essentially characterised by a particular context, and particular circumstances and attitudes, within which information is shared. Ferdinand Schoeman goes further to argue that that the private sphere is essentially a moral sphere, in so far as it encompasses *whatever matters deeply to a person*. A private sphere is a context in which the act of exchanging information is valued, in itself, as a special, meaningful act – regardless of the objective properties of the information (Schoeman, 1984:406). Not the information, but the way in which it is exchanged, defines privacy. It is a context in which the revealer and the recipient of the information play special roles. To the revealer, the information and the act of sharing it with someone else matters deeply. From the recipient is expected a special involvement that anticipates trust and in which they receive the information sympathetically – that is, appreciative of how deeply the information and the act of sharing matters to the revealer. It is by enabling this special context with others that we develop and manage our various intimate relationships (ibid:408) and various dimensions of ourselves (ibid:410). Protecting privacy, then, means protecting this special context. A privacy violation, consequently, means that private information is shared *outside of the appropriate context*.

The particular context, circumstances and attitudes within which people share information are characterised by respect, love, friendship and trust (Fried, 1968:205) and by a dimension of caring (Reiman, 1976:301). The quality or intensity of the private information we exchange with others is not what constitutes the intimacy of our relationship with others – otherwise we would all have very intimate relationships with our doctors and lawyers. Rather, *caring* can be defined as "a reciprocal desire to share present and future intense and important experiences together, not merely to swap information" (ibid:305). It is within a context of caring that the revealing of personal data takes on its private significance. Another, related, characteristic of privacy is *participation*. When we participate in an experience without being observed by others, we are "deeply engrossed" in it, so intensely that the relationship "wholly shapes our consciousness and action" (Gerstein, 1978:77) – an experience that can be likened to that of religious ecstasy. However, as soon as we feel observed by others, we take on their perspective, and feel compelled to adjust our actions – to please the other, or conform with what the other deems right, decent or permissible. Observers merely turn their attention to something or someone from a distance – aloofly, objectively and without participation. We can shift from one perspective to another by losing ourselves in an experience we had been observing up until that point, or by stepping out of an experience we had been deeply engrossed in. This transition is crucial to Gerstein's theory of privacy: as soon as participating turns into observing or into being observed, the intimacy of the experience dissipates. We violate someone's privacy when we involuntarily turn a person who is participating in an experience into the role of an observant. Doing so interferes with their autonomy and liberty to decide for themselves whether to take on a role of participant or that of observer (ibid:78). But the violation does not stop there. Turning a participant involuntarily into an observer interferes with the inherent quality of the experience itself. Not only the participant changes, but the experience changes too – it loses important properties that made it special, meaningful and intimate. The fact that an observer may put their own spin onto the intimate experience they intrude on and misinterpret the intimate significance of the experience for the participants involved, only exacerbates the damage a privacy violation may cause. Gerstein's example of sexual intercourse is illustrative: to be involved in the experience is very different from observing other people being involved in the experience, because observing other people does not give full access to the particular significance the experience has for the participants.

We find a similar conception of privacy violations as a transition from participant to observer perspectives in Stanley Benn's theory of privacy. Our perspective as self-conscious agents with meaningful projects of our own shifts fundamentally when we are observed and judged by others. "Finding oneself an object of scrutiny, as the focus of another's attention, brings one to a new consciousness of oneself, as something seen through another's eyes" (Benn, 1971:227) This new consciousness Benn explains as becoming aware of oneself *as an object.* When observed, a person's "consciousness of pure freedom as subject, as originator and chooser, with infinite, indeterminate possibilities" is transformed into something "fixed, with limited probabilities (…)" (ibid:227).

3.4.2. The moral justification of privacy: the private sphere is a moral sphere

However, while the above descriptions give us a idea of what characterises the private sphere, something is missing – something that is crucial for our moral evaluation of data privacy. Why should a private sphere deserve protection? Why does a context in which values of respect, love, friendship and trust are exchanged deserve protection? What is morally wrong with turning a participant into an observer? What has so far been missing is an argument for the moral justification for privacy. In what follows, I will argue that this justification is motivated by the principle of respect for persons I have introduced earlier.

The principle of respect for persons implies a normative, moral dimension: whatever matters deeply to a person is presumed *good*, deserving of respect and protection, and not to be exploited even for socially or politically worthy ends – for no other reason than the fact that it matters deeply to that person (Schoeman, 1984:415 and 416). The private sphere is therefore, by default, a moral sphere: what matters deeply to one person has "presumptive moral value" over and above whatever matters to anyone else, including what may be regarded as "socially valuable ends" (ibid:415). By protecting privacy, we do not only protect something essential of what it means to be a person, but we also acknowledge the normative moral significance of meaningful social relationships and personal life goals. It is a moral dimension that is essentially reciprocal: by the acknowledgment of ourselves as subjects, we also acknowledge others as conscious subjects with significant projects of their own. Respect for persons then means respecting the principle that every human being is faced with choices that are

important and meaningful to them, because they fundamentally shape their unique individual personhood, and to which they must formulate their own answers. Every person "is entitled to this minimal degree of consideration" (ibid:228), to "experiment with your own life" (Floridi 2014:124). We lose the very concept of a *person* – "it will atrophy and be subsumed by public standards of value" (Schoeman, 1984:414) – if we reduce that person to other people's or social projects. After all, the *personal* relevance of life goals is a crucial aspect of a person's ambitions to pursue these goals, and what matters deeply to one person does not necessarily "gain [its] moral worth through [its] promotion of independently worthy ends" (Schoeman, 1984:404).

Privacy, then, is consistent with the view that all persons have an inherent right to pursue their interests, whatever they may be, as long as they respect this right in everyone else. In other words, privacy does not define *which* projects or relationships need to be valued and protected, but only demands of everyone to respect the equal right of every person to "define and pursue (…) values free from undesired impingements by others" (Fried, 1968:207). In addition to safeguarding the necessary conditions for freely and autonomously designing our personalities and our lives, privacy also provides the necessary context in which we flourish as persons among others: respect, love, friendship and trust (ibid:207). Social relationships that are characterised by these values are not just vague feelings or emotions, but represent a system of dispositions, beliefs and attitudes, organised according to certain principles, and founded on one common conception: the moral conception of personality and the basic entitlements and duties of persons in regard to each other (ibid:206). Privacy is not merely instrumental in bringing about these intimate relationships with others; they are simply inconceivable without privacy or the possibility of privacy. Privacy is the "necessary atmosphere" for our most intimate relationships to even exist "as oxygen is for combustion" (ibid:205 and 477). Moreover, not only are these relationships essential to our integrity as persons, our autonomy and freedom to manage them in varying degrees of intimacy are just as important. The degrees of intimacy we exchange in social relationships constitute "moral capital" (ibid:224). In fact, these different degrees of intimacy are what defines the meaning of our relationships (Rachels, 1975:326, 327) and in turn the meaning of us as persons. We

have therefore good reasons to object to anything that interferes with our freedom to manage our most important social relationships (ibid:329).

We are now in a position to understand why we should not treat (data) privacy violations merely as harm: the moral obligation to respect privacy is first and foremost the obligation to respect persons qua persons, rather than merely a prohibition against harming persons. Publishing private information about someone, or intruding into an intimate relationship, cannot only be judged in terms of harmful consequences. Something of greater moral significance than harm is at stake when the context within which information is shared is disrespected, or when participants are turned into observers. This explains why we may feel that our right to privacy has been violated even when no actual harm can be demonstrated: something has been violated that cannot be expressed in terms of harm. In conclusion, (data) privacy protects something that we value deeply, as persons: our autonomy and freedom to decide for ourselves the context within which we exchange information that matters to us, for no other reason than the fact that it matters to us, because what matters to us defines us as persons, and persons deserve protection.

3.5. Challenges to a value-based approach to data privacy

One may point out that values seem to be nothing more than good consequences, and that a value-based approach to data privacy does therefore not essentially differ from a harm-based approach. It this were true, then it would follow that the criticisms we've raised against a harm-based approach of data privacy in Chapter Two should equally apply to a value-based approach. Or one may even claim that we don't need a concept of privacy at all – we would make things much easier if we'd stick to other, well established moral concepts for the management of our data privacy concerns.

3.5.1. Values are simply good consequences

Perhaps the *good* we aim to establish by promoting values is nothing more than the absence of *harm.* Perhaps we only value what benefits us. Therefore, a value-based approach to data privacy relies on the same presumptions as a harm-based approach: flawed conceptions of what is good, and unreliable predictions of harm and benefits. Aren't definitions of values just

as subjective as definitions of harms? And aren't the practical applications of our values just as unpredictable as the consequences of our actions? If we argue that harm is flawed as a moral approach because it cannot be adequately defined and predicted, then what makes us think that we can define and predict its opposite?

However, harms and values are fundamentally different concepts and it is a mistake to conflate them. Harms materialise in the world as consequences of our actions, and our predictions of harm are (empirically) true or false – either an action causes harm, or it does not (assuming we agree on what constitutes harm). Values, on other hand, do not make predictions, and are not true or false – their moral significance cannot be tested in empirical affirmations or refutations. Rather, values represent our *vision* of how we think the world *ought* to be. We may test our values against the factual state of affairs they give rise to, and test our actions and beliefs for consistency with our values, but the failure to implement our values in the world says nothing about the goodness or badness, or rightness or wrongness, of our values as such. In other words, values derive their meaning and moral significance from desired, or *envisioned*, states of affairs – not from the actual states of affairs they result in or are predicted to result in. In fact, values are insensitive to consequences (Baron and Spranca, 1997:5). This may be what Shaw had in mind when he writes that "value is essentially volitional" (Shaw, 1901:316). Values must be distinguished from consequences that bring about harm or pleasure. We don't only value what benefits us. Whereas harm has reference to the present (what we experience) or to the future (what we don't experience yet, but want to avoid), "value is hampered by no such temporal limits and is thus an unbroken current passing through the act" (ibid:315). To put this differently, values represent something that transcends immediate and future contingencies and realities. In as far as consequences of values ought to be considered, these consequences must not be considered in terms of harm or benefits, but should be considered in relation to the values they represent and implement (ibid:319). The fact that some of our values are in fact in vain, because we struggle to implement them in the world, does not diminish their moral worth.

3.5.2. Value trade-offs are cost-benefit analyses

Nevertheless, as soon as we accept that values deserve protection because they represent our vision of a good world, we run into a problem: not all values are mutually compatible – sometimes value trade-offs are necessary to avoid a moral stalemate or vacuum. Sometimes we need to suspend (part of) the protection of one value to protect another, and "the list of privacy's counterweights is long and growing" (Cohen, 2013:1905). For example, the value of privacy may be at odds with technological innovation and efficiency, the freedom of the press, with the right to access to information, the right to freedom of speech and expression, or with the right to personal security (Kleinig, 2011). Sometimes we may even need to weigh up "privacy-privacy tradeoffs" – for example, when people that deserve privacy protection in one context no longer deserve this protection in another (Gersen, 2022:24-27), or when attempts to protect personal data end up backfiring by drawing more attention to it (Pozen, 2016:222). The latter is best known as the *Streisand effect*, after the famous singer who's legal action to remove an aerial photograph of her house from a website drew unintended global attention to it. One may therefore argue that a value trade-off is nothing more than a cost-benefit analysis: the consequences of protecting one value are simply weighed up against the consequences of protecting another.

But here again we may retort that treating value-trade-offs as consequential cost-benefit analyses ignores the fact that consequences and values are fundamentally different. On the consequentialist view, the moral significance of an action is directly determined by its predicted consequences. On the value-based approach, the moral significance of an action depends on the intrinsic value it represents. This significance is not diminished by our failure to implement the action, or to implement it fully. The value of respect for a human life, for example, does not lose its moral significance in circumstances in which we struggle to protect it, as in cases of famine or war. We might even say that the more obstacles we face to act in accordance with a particularly important value, the stronger our moral obligation to protect it. The same is true of the value of privacy in the current privacy-challenged context.

However, this does not necessarily refute the criticism: even if value trade-offs aren't treated as consequential cost-benefit analyses, they still require us to weigh up and rank values of

different moral significance. How does one go about assigning different weights to values? I suggest that the answer lies in a three-pronged approach, which I discuss in more detail in Section 3.6. below. Relying on Rawls' process of *reflective equilibrium* (Rawls, 1971), I will argue that because data privacy is essentially a value, our ethical judgments about data privacy dilemmas ought to start from a deliberation of values and practical challenges – not from a deliberation of costs and benefits.

Then again, sometimes deliberation may lead to more than one coherent answer, or sometimes to no answers at all – when values of equal weight clash. After all, no set of values is perfectly consistent and coherent, and moral dilemmas are inherent to the nature of ethics. For example, how do we balance principles of privacy with principles of personal security, seeing that both are expressions of the principle of respect for persons? The fundamental right to security of one person may require interference with another's fundamental right to privacy. To resolve this stalemate, I will argue for a *revised* version of Rawls' reflective equilibrium: a rational process of deliberation that seeks to balance abstract notions of morality with practical considerations on the one hand, but that is at all times consistent with the foundational, non-negotiable principle of respect for persons. Referring back to Rescher's terminology, this means that whatever *loci* of values we end up deliberating, the outcome must at all times be consistent with the *underlying* value of the basic respect for every person. This means, essentially, that the principle of respect for persons limits our deliberations, in two ways: (i) outcomes that affect the principle must be rationally argued, in ways that are compatible with our broader framework of morality; and (ii) in the absence of morally defensible reasons to suspend the right to privacy, the outcomes must be subjected to individual consent. But this raises another question: if morality, in the absence of good arguments, ultimately relies on individual consent, how do we know that consent is in itself morally defensible?

3.5.3. When is consent morally defensible?

Not all consent is morally defensible: we may think of many examples where people are manipulated, tempted, misled, or forced into sacrificing a value they hold dear. Consent on its own is not a guarantee for morally defensible outcomes of value-deliberations, and there is no necessary link between consent and autonomy, freedom, well-being and best interests (Eyal,

2019). Violating consent requirements may increase a person's sense of autonomy and well-being – for example, when certain options are taken out of a complicated equation. The requirement of consent may also imply "tortuous deliberations", make us feel unnecessarily responsible for embarrassing mistakes and vulnerable to social pressure, and may conflict with the "principle of beneficence" (Dworkin 1988, ch. 5, in Eyal, 2019). In analogy with performing an emergency medical procedure without a patient's consent, processing personal data without a person's consent does not necessarily violate her best interests. Sometimes the protection of a person's vital[32] or legitimate[33] interests may be sufficient justification to process personal data – for example to prevent harm to a person's health or safety. On the other hand, consent to participate in a dangerous medical experiment, or consent to share personal data without fully understanding the implications of doing so, is not necessarily a sufficient condition to make the experiment or the sharing morally permissible. It is for these reasons that Kant formulates the notion of *rational consent* (Scanlon 1988, in Eyal, 2019). From this perspective, respect for persons means treating them only in ways that they could rationally consent to. In other words, for Kant an action may be morally right even if a person has not in fact consented to it, but other rational people would, and vice versa.

Our modern notion of consent has drifted away from Kant's universal rationality condition towards individual autonomy and freedom. But this does not mean that we no longer rely on universal conditions to distinguish valid from invalid consent. If anything, it has increased the moral significance of individual consent. Consent is *morally transformative* – it "changes the moral relationship between [people] and between them and others" in that it *legitimises* or *obligates* conduct that would otherwise not be permissible or required (Wertheimer, 1996:342). For example, a data subject's consent transforms an impermissible violation of privacy into a permissible exchange of information, and a person's promise to do something transforms their freedom into an obligation to do something. Because the morally transformative aspect of consent can be deeply intrusive, we only deem it morally defensible when expressed *voluntarily* by an *decisionally-capacitated* agent to which *full disclosure* has

[32] Recital 46 GDPR

[33] Section 11(d) POPIA

been made in a manner she *fully understands*. Silence does not constitute consent, and there is no such thing as "presumed consent" (Eyal, 2019).

The question of when consent may be considered valid is extensively worked out in current law on data privacy. Thus we read that consent is valid only if it expresses a person's "voluntary, specific and informed"[34] will in an unambiguously "clear and affirmative act".[35] A person giving consent must "be able to refuse or withdraw consent" at any time (Ustaran, 2019:118-122). This implies that consent can only be valid for as long as it is not withdrawn. Valid consent requires the absence of a "clear imbalance" between the requester and the supplier of consent,[36] and consent may not be "bundled with some other issue" (ibid:118). When consent is requested in a context "which also concerns other matters" (for example, in exchange for goods and services) then the request must be "clearly distinguishable" from these other matters[37] and may only be required if it is strictly "necessary for the performance of a contract" (ibid:119). It may only be requested and given for a specific purpose, which must be clearly explained by the requester, and if that purpose changes after consent has been given, a renewed consent must be requested for the renewed purpose. This ties in directly with the need for transparency and information: consent is only valid if it is given by a person that has access to "all the necessary details (…) in a language and form they can understand so that they can comprehend how [consenting] will affect them" and has been given a "reasonable opportunity to be informed of the significance of this consent" (ibid:121).

3.5.4. Privacy as a separate value is redundant

While the above challenges may be applied to any value-based morality, another challenge has been raised specifically in respect of privacy: perhaps we do not need a distinct concept of privacy to protect its concerns, we have other instruments that perfectly cover that protection. Moral justifications for privacy were increasingly founded on the notion of protection of individual property rights from the early modern period (roughly 1500 CE). Today's widely

[34] Section 1 POPIA

[35] Recital 32 and Article 4(11) GDPR

[36] Recital 43 GDPR

[37] Article 7 GDPR

shared view that people have property rights over information that relates to them can be traced back to John Locke's conception of property rights as natural rights (Solove, 2002:1112) which claim that every person "has a property in his own person (…)"[38]. It is during this time (1604) that the ruling *the house of everyone is his castle* is coined for the first time (DeBrabander, 2020:78-88) – which was initially a protection of citizens against intrusions of the state. It is a view that prompts Judith Jarvis Thomson to argue that we don't need a separate right to privacy (Thomson, 1975:306) – as I have briefly discussed in Chapter One.

However, the argument against privacy as a separate value worth protecting in its own right is flawed in a number of respects. For one thing, reducing privacy rights to property rights is not at all helpful to explain and resolve complex moral dilemmas, for example between the right to privacy and freedom of expression and press. Property rights may be relevant to determine the boundaries of our "zone of privacy" (Scanlon, 1975:318), but privacy concerns are distinctly unified by a "common foundation in the special interests that we have in being able to be free from certain kinds of intrusions" (ibid:315). In support of Scanlon's argument, Ferdinand Schoeman asks us to imagine two distinct technologies (Schoeman, 1984:27). Both record the sound waves produced by a person's voice, but one records the actual verbal content carried by the sound waves, whereas the other converts the sound waves into useful energy but makes no record of the content. Our privacy concerns in the first scenario may be explained by the violation of property rights, argues Schoeman, but what about the second scenario? Assuming that people do indeed own the sound and contents their voices produce, do they also have a property claim to whatever is done with that sound – especially if that sound is converted in a way that can no longer identity them. Schoeman thinks not – we no longer have a property claim to energy that is made from our voice recordings – but that does not mean that we are no longer concerned about the use of our voice recordings. This, argues Schoeman, proves that we have privacy interests that are distinct from property rights.

However, even if we concede that privacy concerns are not reducible to property rights, we still need a positive account of what motivates or justifies these concerns. Jeffrey Reiman

[38] §27 of Two Treatises of Government, 1689

offers the most direct reply: privacy isn't a derivative of property rights; instead, property rights are expressions of the right to privacy (Reiman, 1976, in Schoeman:301). Justifications for protecting personal property are preceded by justifications to protect persons *qua* persons. In other words, before we assign people the right to own personal property, we assign them the right to be a person, and to be respected as a person. Part of being a person is being able to maintain social relationships of different degrees of intimacy with different people (Fried, 1968:475; Rachels, 1975:326). The circumstances within which we exchange love, friendship and trust, or reveal information about us or private body parts to other people has nothing to do with property rights or rights to the person (we don't exchange property rights to our bodies or our person with other people), but are defined by the social relationship that provides the context for these revelations. The fact that we do reveal them in certain contexts and not in others, proves the point that privacy is motivated by how we autonomously manage the intimacy of these contexts – not by property claims. It should be clear then, that property rights may be helpful in the protection of privacy, but property rights are an expression of the underlying justifications for privacy – not the other way round. As it turns out, this argument is remarkably relevant for today's debate around the issues of data privacy, in which some argue that people stop having ownership claims over their own personal data once this information is turned into anonymous algorithmic data that powers new technologies (Gilbert, 2021:21, 22, and 28).

3.6. Application of a value-based approach to data privacy

The aim of this thesis is not only to gain an understanding of what data privacy is, and why it deserves protection, but also to make suggestions on how we may go about this protection. I have argued that data privacy constitutes the necessary context to respect persons qua persons. In other words, data privacy is a value that deserves protection because it is a necessary condition for the protection of another, foundational, underlying value: the principle of respect for persons. I have also argued that, because our concepts and predictions of harm are unreliable in a rapidly evolving technological context, it would be wrong to treat the value of data privacy solely in terms of harms and benefits. Rather, it must be deliberated rationally in relation to other values and practical considerations. And lastly, I have argued that any outcomes of our deliberations must at all times be respectful of persons. Moral decisions that

can be argued rationally but ignore the principle of respect for persons without good reasons, or for reasons that are incompatible with our broader framework of morality, are indefensible in liberal democracies. In this section, I discuss different ways in which we may deliberate and apply values, defend one particular procedure, and apply this procedure to a recent example of a global data privacy dilemma.

A deliberation of values may be approached from three directions: top-down, bottom-up, or a combination of both. The first approach attempts to capture moral concerns in abstract notions that serve as justifications for our practical judgements. For example, we may prohibit certain practical applications of new technologies because they go against our established moral conceptions of privacy. But there is an obvious problem with this approach: it may feel disconnected from reality – utopian, as if moral values represent a perfectly coherent world that is detached from the practical circumstances and challenges they apply to. More specifically, a top-down approach struggles to account for complex privacy challenges in an unprecedented and rapidly changing technological context. Rather than shedding light on our moral concerns around data privacy, theories of privacy that attempt to formulate perfectly coherent, abstract, top-down conceptions of privacy seem to do little more than confounding the various issues at stake with deeply challenging and contradictory claims (Parent, 1983:341), and often turn out to be "practically useless" (Solove, 2015:73).

The opposite of a top-down approach is a bottom-up approach – or what is generally referred to in the study of applied ethics as the case study method. In fact, this "pragmatic", "bottom-up, contextualised" approach may be the best possible approach in an era of unprecedented, rapidly changing technology (Solove, 2002:1091 and 1154). Rather than attempting to formulate generally applicable theories of privacy, this approach attempts to extract moral notions from the study of practical moral judgements. It treats moral questions "as being implicit in the activity of agents rather than explicitly articulated (or even articulatable) in terms of a general theory" (Wallach, Allen, Smit, 2005). Much like legal scholars study the practical reasoning behind judicial case law, case ethics studies the practical reasoning that underlies our moral judgements, and how that reasoning relates to more general principles (Darwall, 2005:18). But there are problems with this approach too: its pragmatic attempts to

distill moral claims from factual circumstances and judgements may detach us from our abstract notions of moral value. More importantly, claims about what *ought to be* cannot be based solely on statements about what *is*. Meta founder Mark Zuckerberg famously expressed the old philosophical *is-ought* problem when he first rejected and later defended privacy on the basis of social practices."[39] Contrary to the *Theory of Technological Determinism*, our vision of the good life ultimately determines how technology develops – not the other way round. But then the question remains: how do we make sure that we take into account practical circumstances (including those enabled by new technologies) while safeguarding our most important moral values?

Rather than opting for either a top-down or bottom-up approach, I propose that we reason moral concerns around data privacy "from both ends (…) going back and forth" (Rawls, 1971:18) – or or up and down, if you wish – between our values on the one hand and practical moral challenges on the other. This method of ethical reasoning is known as *reflective equilibrium* (Rawls, 1971; Archard and Lippert-Rasmussen, 2013:3 and 11). What the method is after, is an *equilibrium* between all moral values and practical judgements that are at play when data privacy is at stake. But not just any equilibrium will do – it must be a process of *reflective* deliberation. Whether moral values and practical judgements do in fact cohere is subject to rational deliberation of consistency and coherence within a broader moral framework (Archard and Lippert-Rasmussen, 2013:3 and 11) that provides a context in which one value supports or provides the best explanation for other values (Daniel, 2020). In other words, the protection of data privacy and its underlying principle of respect for persons must be coherent with the protection of other values, while taking into account changing practical circumstances.

However, even when we acknowledge the multitude of values and practical circumstances that is at stake in our data privacy concerns and set out to find coherent practical answers, we may view some values as non-negotiable and not up for revision, whatever the consequences

[39] Both quotations belong to Facebook founder Marc Zuckerberg, who in 2014 stated that "Privacy [is] no longer a social norm (…)" (theguardian.com/technology/2010/jan/11/facebook-privacy) and later in 2019 changed his tune to "the future is private" (Véliz, 2020:44).

(Baron and Spranca, 1997:1-3). The moral obligation to act in accordance with these values is not a matter of personal preference, convention, or negotiation, but is absolute (ibid:5). It is an obligation that is so pervasive that its violation leads to moral outrage (ibid:6). Because of the foundational role it plays in liberal democracies, I argue that the principle of respect for persons is one of those values. Therefore, the particular approach of reflective equilibrium I argue for is known as foundationalist, as it rests on a non-negotiable principle that sets clear boundaries for moral deliberation of data privacy concerns (Daniels, 2020).

The three-pronged approach I suggest, starts with a reflective deliberation of values and practical challenges, tests the outcome of our deliberations against the principle of respect for persons, and ends, in the absence of conclusive outcomes, with individual consent. We may illustrate this with a recent example of a global data privacy dilemma: contact-tracing technology. Whether or not this technology, like we have seen during the Covid-19 pandemic, is morally defensible, depends, firstly on the outcome of our reflective deliberation of values and practical challenges. These include the moral obligation to contribute to, or at least not obstruct human collective welfare and wellbeing, versus the moral obligation to protect people's autonomy and freedom, as well as practical considerations such as the nature of the data that is collected and the ways in which it is processed, the need for a certain number of people to share data for the technology to work, the particular urgency and uncertainty that surrounded the pandemic, and the negative impact on society, the economy, and the public healthcare system. Next, contact-tracing technology must be held against the principle of respect for persons, which is represented here by the right to privacy: does tracking people's location and Covid status, as well as the network of people they interact with, violate privacy rights? Seeing that Bluetooth-based contact-tracing mobile applications do not collect identifiable personal data, or data that may be re-identified by reasonably foreseeable methods in the future, we may reply that the technology is in fact compatible with the principle of respect for persons. To the claim that we don't know which data will be re-identified by future technologies, we may reply that a rational balance of the right to privacy with the other moral and practical concerns listed above, would argue in favour of contact-tracing: there are no rational arguments for accepting that the data can be re-identified, and the offhand chance of this happening in the future does not weigh up against our other imminent concerns. On the

other hand, should it be so that contact-tracing technology does in fact process personal data, then the principle of respect for persons will demand that extra safeguards are put in place, which allows people to consent or object. However, we may think of other applications of the technology that automatically fail the test: publicly surveilling people, implanting tracking devices in people, or installing tracking technology on people's wearable or mobile devices, by means of which people's identifiable biometric data can be monitored without their consent. This is where the principle of respect for persons draws the line between morally defensible and morally indefensible outcomes of our deliberations: while there may be a clear moral obligation to contribute data to contact-tracing technology, applying the technology without people's consent would violate the principle of respect for persons – it would be immoral.

3.7. Conclusion

The method I propose for managing data privacy is based on my arguments for why it deserves protection. Before I have set out these arguments in this final chapter, I have looked at what moral values are and why we protect them. I have also introduced the particular moral value my arguments will rely on: the liberal ideal of respect for persons. Next, I have set out my arguments for data privacy in two steps. First, I have defined privacy, including data privacy, as a unique context in which we share experiences and information that matter to us. Second, I have argued that this context deserves protection because it constitutes a necessary condition for the protection of persons qua persons. In reply to potential criticisms, I have argued that because values are fundamentally different from beneficial consequences, and value deliberations are different from cost-benefit analyses, the criticisms I had raised in Chapter Two do not apply to the value-based approach to data privacy I defend here. In addition, I have shown how the protection of persons may require us to subject our moral deliberations to valid individual consent. And lastly I have argued against the claim that we don't need a concept of privacy to protect its moral concerns.

After having set out my arguments, I have proposed a revised, three-pronged version of Rawls' reflective equilibrium to manage data privacy, and applied it to the example of contact-tracing technology. First, we list and rank all moral values as well as practical concerns that

are at stake. Second, we try and find a rationally argued, coherent balance between these values, concerns, and the principle of respect for persons. And three, in case no conclusive outcomes can be reached, we subject data privacy challenges to valid individual consent.

CONCLUSION

At the start of this thesis I have set out to formulate answers to three questions: what is data privacy, why does it deserve protection, and how should we go about managing this protection? These questions are commonly known in the study of applied ethics as conceptual, normative, and practical: a conceptual analysis defines the building blocks and moral landscape of our issue at hand; a normative analysis argues for or against a particular justification for protecting or rejecting our moral concern; and a practical analysis looks at how we may apply our conceptual and normative findings to real moral dilemmas in the field.

To the first question I have replied that data privacy is characterised by a coherent set of concerns with an intrinsic moral value, distinct from other moral concern and from concerns we have faced in the past. I have tentatively defined data privacy as *measures and tools that aim to control how data about identifiable people is processed by ICT.* Following this, I have examined two possible justifications for data privacy: a harm-based and a value-based justification. The harm-based approach, I have argued, rests on flawed assumptions about our ability to define harm and to predict its occurrence, however defined. These flaws become magnified in the context of a rapidly changing Information Society. My argument for an alternative approach is based on the claim that (data) privacy is a value, and ought to be treated as such. In addition, I have explained why values deserve protection, and why we expect them to be consistent and coherent with our broader ethical framework. Central to this argument is the claim that privacy is not merely an instrumental good, but an intrinsic value that is co-constitutive of *respect for persons*. Privacy, in other words, cannot be replaced by any other instrument that aims to uphold the principle of respect for persons. This has direct implications for the moral significance of privacy: whatever matters deeply to a person has moral significance for the person(s) involved as well as for anyone intending to interfere, over and above any other concerns.

However, attempting to reply to the third question reveals a problem: simply relying on a non-negotiable principle of respect for persons may not always produce the best answers to our moral dilemmas. All too often, one person's moral concerns are at loggerheads with other

people's concerns, and a deliberation of opposing values is necessary to avoid a moral stalemate. I have suggested a three-pronged approach that acknowledges, ranks, and deliberates on all values that are at stake, with the aim of attaining a foundationalist version of reflective equilibrium, in which all values and practical considerations are consistently and coherently in balance with our broader moral framework, but ultimately subjected to the value of each and every person to decide what matters for themselves.

REFERENCES

Allen, A.L. (2000). *Gender and Privacy in Cyberspace*. Stanford Law Review, May, 2000. pp. 1175-1200. Available at www.jstor.org/stable/1229512

Anderson, E. (1993). *Value in Ethics and* Economics. Harvard University Press: Cambridge, Massachusetts. Available at nissenbaum.tech.cornell.edu/papers/Anderson.pdf

Andrejevic, M. (2014). *Big Data, Big Questions. The Big Data Divide*. International Journal of Communication, [S.l.], v. 8, p. 17, jun. 2014. ISSN 1932-8036. Available at: ijoc.org/index.php/ijoc/article/view/2161/1163. Date accessed: 06 Sep. 2021

Archard, D. and **Lippert-Rasmussen**, K. (2013). *Applied Ethics*. The International Encyclopedia of Ethics, First Edition. Edited by Hugh LaFollette. Blackwell Publishing Ltd. DOI: 10.1002/9781444367072.wbiee693. Available at www.researchgate.net/publication/315701468

Baron, J. (2017). *Protected Values and Other Types of Values*. Analyse & Kritik 2017; 39(1): 85–99. Available at analyse-und-kritik.net/Dateien/5dfbb50bf01d0_baron.pdf

Baron, J. and **Spranca**, M. (1997). *Protected Values*. Organizational Behavior and Human Decision Processes Vol. 70, No. 1, April, Pp. 1–16, 1997. Article No. Ob972690. Available at sas.upenn.edu/~baron/papers/pv97.pdf

Bell, D. (2020). *Communitarianism.* The Stanford Encyclopedia of Philosophy (Fall 2020 Edition), Edward N. Zalta (ed.), Available at plato.stanford.edu/archives/fall2020/entries/communitarianism

Benn, S. I. (1971). *Privacy, freedom, and respect for persons.* Lieber-Atherton, Inc., in Schoeman, F. (2007). *Philosophical dimensions of privacy. An anthology*. Cambridge University Press: Cambridge. Re-issued digitally printed version. pp. 223-243

Bimber, B. (1990). *Karl Marx and the Three Faces of Technological Determinism*. Social Studies of Science, 20(2), 333–351. Available at www.jstor.org/stable/285094

Blackburn, S. (2016). *The Oxford Dictionary of Philosophy.* Oxford : Oxford University Press

Blitz, M. (2014). *Understanding Heidegger on Technology*. The New Atlantis, 41, 63–80. Available at www.jstor.org/stable/43152781

Bloustein, E. J. (1964). *Privacy as an aspect of human dignity: an answer to Dean Prosser*. New York University Law Review, 1964. Reprinted from New York University Law Review 39: 962-1007, 196 in Schoeman, F. (2007). *Philosophical dimensions of privacy. An anthology*. Cambridge University Press: Cambridge. Re-issued digitally printed version. pp. 156-202

Bradley, B. (2012). *Doing Away with Harm.* Philosophy and Phenomenological Research, 85(2), 390–412. Available at www.jstor.org/stable/41721239

Branscomb, A.W. (1994). *Who Owns Information? From Privacy to Public Access*. Basic Books, New York

Brin, D. (1998). *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* Reading, MA: Addison-Wesley. Harvard Journal of Law & Technology, Vol. 12, No. 2

Brink, D. (2022). *Mill's Moral and Political Philosophy.* The Stanford Encyclopedia of Philosophy (Spring 2022 Edition), Edward N. Zalta (ed.), forthcoming. Available at plato.stanford.edu/archives/spr2022/entries/mill-moral-political/

Chandler, D. (1995). *Technological or Media Determinism*. Available at www.wolearn.org/pluginfile.php/45/mod_page/content/23/chandler2002_PDF_full.pdf

Crimmins, J. E. (2021). *Jeremy Bentham.* The Stanford Encyclopedia of Philosophy (Winter 2021 Edition), Edward N. Zalta (ed.), Available at plato.stanford.edu/archives/win2021/entries/bentham

Cohen, J.E. (2013). *What Privacy Is For.* Vol. 126 Harvard Law Review, pp1904-1933

Courtland, S.D., **Gaus**, G. and **Schmidtz**, D. (2022). *Liberalism*, in The Stanford Encyclopedia of Philosophy (Spring 2022 Edition), Edward N. Zalta (ed.), forthcoming. Available at plato.stanford.edu/archives/spr2022/entries/liberalism

Daniels, N. (2020). *Reflective Equilibrium*. The Stanford Encyclopedia of Philosophy (Summer 2020 Edition), Edward N. Zalta (ed.). Available at plato.stanford.edu/archives/sum2020/entries/reflective-equilibrium/

DeBrabander, F. (2020). *Life after Privacy, Reclaiming Democracy in a Surveillance Society.* Cambridge : Cambridge University Press (Kindle edition)

de Stadler, E., **Luttig Hattingh**, I., **Esselaar**, P., **Boast**, J. (2021). *Over-thinking the Protection of Personal Information Act*. Cape Town : Juta and Company (Pty) Ltd.

de Villiers-Botha, T. (2020). *Harm as Negative Prudential Value: A Non-Comparative Account of Harm*. SATS, Vol. 21 (Issue 1), pp. 21-38. https://doi.org/10.1515/sats-2019-0025

Darwall, S.L. (2005). *Theories of Ethics*. A Companion to Applied Ethics. Edited by R.G. Frey and Christopher Heath Wellman. Blackwell Publishing

DeCew, J. (2018). *Privacy.* The Stanford Encyclopedia of Philosophy (Spring 2018 Edition), Edward N. Zalta (ed.). Available at plato.stanford.edu/archives/spr2018/entries/privacy

Dewey, J. (1939). *Theory of valuation*. Chicago, Ill., The University of Chicago Press

Dillon, R. S. (2020). *Respect.* The Stanford Encyclopedia of Philosophy (Summer 2021 Edition), Edward N. Zalta (ed.). Available at plato.stanford.edu/archives/sum2021/entries/respect/

Edel, A. (1953). *Concept of Values in Contemporary Philosophical Value Theory*. The University of Chicago Press on behalf of the Philosophy of Science Association. Philosophy of Science , Jul., 1953, Vol. 20, No. 3 (Jul., 1953), pp. 198-207. Available at jstor.org/stable/185497

Eyal, N. (2019). *Informed Consent.* The Stanford Encyclopedia of Philosophy (Spring 2019 Edition), Edward N. Zalta (ed.). Available at https://plato.stanford.edu/archives/spr2019/entries/informed-consent/.

Etzioni, A. (1999). *The Limits of Privacy*. Contemporary Debates in Applied Ethics, A.I. Cohen and C.h. Wellman (eds.). Blackwell Publishing (2005) Chapter 17, pp. 253-262

Etzioni, A. (2014). *The Limits of Transparency*. Public Administration Review, Vol. 74, No. 6, pp. 687-688. Available at www.jstor.com/stable/24029489

Floridi, L. (2013). *The Ethics of Information*. Oxford : Oxford University Press (Kindle Edition)

Floridi, L. (2014). *The Fourth Revolution: How the Infosphere is Reshaping Human Reality*. Oxford : Oxford University Press (Kindle Edition)

Floridi, L. (2015). *The Onlife Manifesto - Being Human in a Hyperconnected Era*. London : Springer Open. Available at: academia.edu/9742506/ [Accessed 19 October 2020]

Foglia, M. and **Ferrari**, E. (2019). *Michel de Montaigne.* The Stanford Encyclopedia of Philosophy (Winter 2019 Edition), Edward N. Zalta (ed.), Available at plato.stanford.edu/archives/win2019/entries/montaigne

Fried, C. (1968). *Privacy*. The Yale Law Journal, Vol. 77, No. 3. Available at www.jstor.org/stable/794941

Friedman, D.D. (2005). *The Case for Privacy.* Contemporary Debates in Applied Ethics, A.I. Cohen and C.h. Wellman (eds.). Blackwell Publishing (2005) Chapter 17, pp. 263-275

Gersen, J.S. (2022). *Keep Out*. The New Yorker. Annals of Law. June 27, 2022

Gerstein, R.S. (1978). *Intimacy and Privacy*. The University of Chicago Press. Available at www.jstor.org/stable/2380133

Gert, B. and **Gert,** J. (2020). *The Definition of Morality.* The Stanford Encyclopedia of Philosophy (Fall 2020 Edition), Edward N. Zalta (ed.), Available at plato.stanford.edu/archives/fall2020/entries/morality-definition/

Gilbert, S. (2021). *Good Data: An Optimist's Guide to Our Digital Future*. Welbeck Publishing (Kindle edition)

Green, J. and **Shariff,** A. (2021). *Our evolved intuitions about privacy aren't made for this era*. Available at www.psyche.co/ideas/our-evolved-intuitions-about-privacy-arent-made-for-this-era

Habermas, J. (1998). *Between Facts and Norms: Contributors to a Discourse Theory of Law and Democracy*, translated by William Rehg. Cambridge: MIT Press

Habibi, D. (1996). *J. S. Mill's Grand, Leading Principle*. The Jerusalem Philosophical Quarterly, S. H. Bergman Center for Philosophical Studies, pp 79-104. Available at www.jstor.org/stable/23350976

Hansson, S.O. (2013). *Fair Exchanges of Risk*. In: The Ethics of Risk. Palgrave Macmillan, London. Available at https://doi.org/10.1057/9781137333650_7 [Accessed 22 March 2021] pp 97-110

Hansson, S.O. (2018). *How to Perform an Ethical Risk Analysis (eRA)*. Risk Analysis. Vol. 38 No 9, 2018. DOI: 10.1111/risa.12978.

Harari, Y. N. (2015). *Sapiens: A Brief History of Humankind*. Random House. Kindle Edition

Harman, E. (2009). *Harming as Causing Harm.* in Roberts and Wasserman (eds.), Harming Future Persons , pp. 137. Available at www.princeton.edu/~eharman/HarmingAsCausingHarm.pdf

Hartmann, N. (1932). *Ethics*. Authorized translation by Stanton Coit. 3 Volumes. New York, The Macmillan Company, 1932. Pp. 344; 476; 2

Hauer,T. (2017). *Technological determinism and new media*. International Journal of English, Literature and Social Science (IJELS). Vol-2, Issue-2, Mar-Apr- 2017

Holvast, J. (2009). *History of Privacy*, in V. Matyáš et al. (Eds.): The Future of Identity, IFIP AICT 298, pp. 13–42, 2009. © IFIP International Federation for Information Processing

Johnson, R. and **Cureton**, A. (2022). *Kant's Moral Philosophy.* The Stanford Encyclopedia of Philosophy (Spring 2022 Edition), Edward N. Zalta (ed.), plato.stanford.edu/archives/spr2022/entries/kant-moral

Kasper, D. V. S. (2007). *Privacy as a Social Good*. Social Thought & Research , 2007, Vol. 28, Social "Movements", pp. 165-189. Available at www.jstor.org/stable/23252125

Kahneman, D. (2011). *Thinking fast and slow*. Farrar, Straus and Giroux. USA

Kleinig, J, et al. (2011). *Securitization Technologies. Security and Privacy: Global Standards for Ethical Identity Management in Contemporary Liberal Democratic States.* ANU Press, 2011, pp. 89–128. Available at jstor.org/stable/j.ctt24h8h5.11

Leonelli, S. (2020). *Scientific Research and Big Data*, The Stanford Encyclopedia of Philosophy (Summer 2020 Edition), Edward N. Zalta (ed.), Available at: plato.stanford.edu/

MacKinnon, C. (1989). *Toward a Feminist Theory of the State.* Cambridge, MA: Harvard University Press. Available at https://books.google.co.za/books?id=Shn5xHywtHIC

Magi, T. J. (2011). *Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature.* The Library Quarterly: Information, Community, Policy, Vol. 81, No. 2, pp. 187-209. Available at www.jstor.org/stable/10.1086/658870

Magidor, O. (2020). *Category Mistakes.* The Stanford Encyclopedia of Philosophy (Winter 2020 Edition), Edward N. Zalta (ed.). Available at plato.stanford.edu/archives/win2020/entries/category-mistakes/

Merton, R. K. (1968). Social Theory and Social Structure. New York:Free Press.

Mill, J.S. (1863). *Utilitarianism*. In Shafer-Landau, R. (2013). *Ethical Theory: An Anthology*, second edition. John Wiley & Sons Inc : West Sussex, pp 417-422

Moore, G. E. (1903). *Principia Ethica*. Cambridge: Cambridge University Press

Moore, A.D. (2012). *Privacy*. Available at www.researchgate.net/publication/228227066

Murphy, R. F. (1964). *Social distance and the veil.* American Anthropologist 66(6) Pt. 1, pp. 1257-74. American Anthropological Association, in Schoeman, F. (2007). *Philosophical*

dimensions of privacy. An anthology. Cambridge University Press: Cambridge. Re-issued digitally printed version. pp. 34-55

Parent, W.A. (1983). *Recent Work on the Concept of Privacy*, in American Philosophical Quarterly, University of Illinois Press on behalf of the North American Philosophical Publications, Vol. 20, No. 4, pp. 341-355

Perry, R.B. (1954). *General Theory of Value, Its Meaning and Basic Principles Construed in Terms of Interest*. Harvard University Press.

Posner, R.A. (1978). *An economic theory of privacy*. American Enterprise Institute, 1978. Reprinted from Regulation (May/June): 19-26, 1978, in Schoeman, F. (2007). *Philosophical dimensions of privacy. An anthology*. Cambridge University Press: Cambridge. Re-issued digitally printed version. pp. 333-345

Powell, T. R. (1913). *The Study of Moral Judgments by the Case Method*. The Journal of Philosophy, Psychology and Scientific Methods, 10(18), 484–494. https://doi.org/10.2307/2013558

Prosser, W.L. (1960). *Privacy*. California Law Review, Vol. 48, No. 3. California Law Review, Inc. Available at www.jstor.org/stable/3478805

Pozen, D. E. (2016). *Privacy-Privacy Tradeoffs*. The University of Chicago Law Review, 83(1), 221–247. http://www.jstor.org/stable/43741598

Rachels, J. (1975). *Why Privacy is Important*. Philosophy and Public Affairs, Vol. 4, No. 4. Blackwell Publishing. Available at www.jstor.org/stable/2265077

Rawls, J. (1971). *A Theory of Justice.* Revised Edition. The Belknap Press of Harvard University Press Cambridge, Massachusetts.

Rescher, N. (1969). *Introduction to Value Theory*. Englewood Cliffs: Prentice Hall, pp. 1-12.

Reinsel, D., **Gantz**, J. and **Rydning**, J. (2018). *The Digitization of the World, From Edge to Core*. IDC White Paper. The International Data Corporation. Available at seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

Reiman, J.H. (1976). *Privacy, Intimacy, and Personhood.* Philosophy and Public Affairs, Vol. 6, No. 1. Blackwell Publishing. Available at www.jstor.org/stable/2265060

Ritov, I. and **Baron**, J. (1999). *Protected Values and Omission Bias*. Available at www.sas.upenn.edu/~baron/papers/pvom.pdf

Rosen, G. (2003). *Culpability and Ignorance.* Proceedings of the Aristotelian Society, vol. 103, 2003, pp. 61–84. JSTOR, Available at jstor.org/stable/4545386

Rudy-Hiller, F. (2018). *The Epistemic Condition for Moral Responsibility.* The Stanford Encyclopedia of Philosophy (Fall 2018 Edition), Edward N. Zalta (ed.), Available at plato.stanford.edu/archives/fall2018/entries/moral-responsibility-epistemic/

Scanlon, T. (1975). *Thomson on Privacy*. Philosophy and Public Affairs, Vol. 4, No. 4. Blackwell Publishing. Available at www.jstor.org/stable/2265076

Schoeman, F. (1984). *Philosophical dimensions of privacy. An anthology*. Cambridge University Press: Cambridge. First published in 1984. Re-issued in digitally printed version in 2007

Schroeder, M. (2021). *Value Theory.* The Stanford Encyclopedia of Philosophy (Fall 2021 Edition), Edward N. Zalta (ed.). Available at plato.stanford.edu/archives/fall2021/entries/value-theory

Sinnott-Armstrong, W. (2021). *Consequentialism*. The Stanford Encyclopedia of Philosophy (Fall 2021 Edition), Edward N. Zalta (ed.). Available at plato.stanford.edu/archives/fall2021/entries/consequentialism

Smith, H. (1983). *Culpable Ignorance*. The Philosophical Review, vol. 92, no. 4, 1983, pp. 543–571. Available at jstor.org/stable/2184880. [Accessed 16 May 2021]

Solove, D. J. (2002). *Conceptualizing Privacy.* California Law Review, Vol. 90, No. 4, pp. 1087-1155. Available at www.jstor.org/stable/3481326

Solove, D. J. (2015). *The meaning and value of privacy,* in Roessler, B. and Mokrosinska, D. (eds) Social Dimensions of Privacy: Interdisciplinary Perspectives. Cambridge: Cambridge University Press, pp. 71–82. doi: 10.1017/CBO9781107280557.005.

Stake, R. E. (1978). *The Case Study Method in Social Inquiry*. Educational Researcher, 7(2), 5–8. https://doi.org/10.2307/1174340

Stanton-Ife, J. (2022). *The Limits of Law*. The Stanford Encyclopedia of Philosophy (Spring 2022 Edition), Edward N. Zalta (ed.), forthcoming. Available at www.plato.stanford.edu/archives/spr2022/entries/law-limits/

Stevenson, C. L. (1944). *Ethics and Language*. New Haven: Yale University Press

Swanson, J.A. (1992). *The Public and the Private in Aristotle's Political Philosophy*. Cornell University Press. Available at www.jstor.org/stable/10.7591/j.ctvn1t9wp.5

Thomson, J.J. (1975). *The Right to Privacy*. Philosophy and Public Affairs, Vol. 4, No. 4. Princeton University Press. Available at www.jstor.org/stable/2265075

Torra, V., **Navarro-Arribas**, G (2014). *Data privacy*. WIREs Data Mining and Knowledge Discovery. pp 269-280. https://doi.org/10.1002/widm.1129

Urban, W. M. (1930). *Fundamentals of Ethics*. New York: Henry Holt and Co.

Ustaran, E. and others (2019). *European Data Protection Law and Practice*, second edition. The International Association of Privacy Professionals (IAAP). Portsmouth USA

Vallor, S. (2016). *Technology and the Virtues*. Oxford University Press. Kindle Edition.

Vanderheiden, S. (2016). *The Obligation to Know: Information and the Burdens of Citizenship*. Ethical Theory and Moral Practice, vol. 19, no. 2, 2016, pp. 297–311., Available at jstor.org/stable/24762628. [Accessed 16 May 2021]

Véliz, C. (2020). *Privacy is Power. Why and How You Should Take Back Control of Your Data*. Transworld. Bantam Press. ISBN 9781787634046 (Kindle Edition)

Véliz, C. (2022). *Self-Presentation and Privacy Online.* Journal of Practical Ethics 9(2). doi: https://doi.org/10.3998/jpe.2379

Warren, S.D. and **Brandeis**, L.D. (1890). *The Right to Privacy*. Harvard Law Review, Vol. 4, No. 5. pp. 193-220. The Harvard Law Review Association. Available at www.jstor.org/stable/1321160

Wasserstrom, R. A. (1978). *Privacy, some arguments and assumptions*. Greenwood Press, Westport, Connecticut from *Philosophical Law*, in Schoeman, F. (2007). *Philosophical dimensions of privacy. An anthology*. Cambridge University Press: Cambridge. Re-issued digitally printed version. pp. 317-332

Wallach, **W. Allen C.** and **Smit, I.** (2005). *Machine Morality: Bottom-up and Top-down Approaches for Modeling Human Moral Faculties.* The Association for the Advancement of Artificial Intelligence. Available at www.aaai.org/Papers/Symposia/Fall/2005/FS-05-06/FS05-06-015.pdf

Wertheimer, A. (1996). *Consent and Sexual Relations*. Cambridge University Press. Legal Theory 2:2 (1996): 89–112.

Westin, A. F. (1967). *The Origins of Modern Claims to Privacy* in Privacy and Freedom. The Association of the Bar of the City of New York, in Schoeman, F. (2007). *Philosophical*

dimensions of privacy. An anthology. Cambridge University Press: Cambridge. Re-issued digitally printed version. pp. 56-71

Wilson, E.O. (2017). *The Origins of Creativity*. Liveright : New York

Zuboff, S. (2019). *The Age of Surveillance Capitalism*. Profile Books Ltd : London (Kindle Edition)

Zuboff, S. (2019). *High tech is watching you.* The Harvard Gazette. Available at news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/